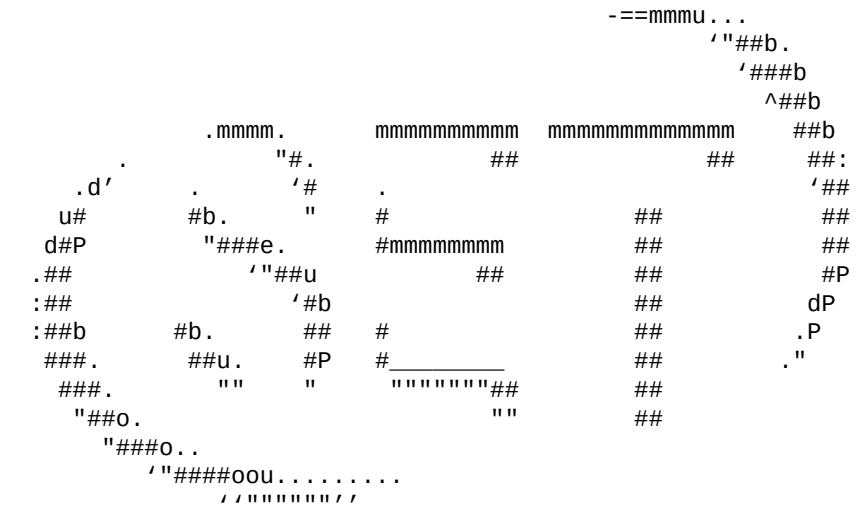


Saqueadores Edicion Tecnica

INFORMACION LIBRE PARA GENTE LIBRE

SET #26 - 30 de octubre de 2002

EDITORIAL

SET Ezine

Disponible en:
    http://www.set-ezine.org

Mirrors:
    http://salteadores.tsx.org
    http://www.zine-store.com.ar

Contacto:
    <web@set-ezine.org>
    <set-fw@bigfoot.com>

AVISO

ADVERTENCIAS

* La INFORMACION contenida en este ezine no refleja la opinion de nadie y se facilita con caracter de mero entretenimiento, todos los datos aqui presentes pueden ser erroneos, malintencionados, inexplicables o carentes de sentido.
El GRUPO SET no se responsabiliza ni de la opinion ni de los contenidos de los articulos firmados.
De aqui EN ADELANTE cualquier cosa que pase es responsabilidad vuestra. Protestas dirigirse a /dev/echo o al tlf. 900-666-000

-----[TABLA DE CONTENIDOS]----
----[SET 26]----

"Los videojuegos no afectan a los ninyos. Si fuera asi y el comecocos nos hubiera afectado a nosotros cuando eramos ninyos, ahora estariamos deambulando por lugares oscuros, comiendo pildoras magicas y escuchando ritmos electronicos repetitivos."

Kristian Wilson, Nintendo, Inc, 1989

EOF

-[0x01]--
-[Editorial]---
-[by Editor]---SET-26--

Veintiseis numeros ya, desde luego, a primera vista veintiseis numeros no parece demasiado, y todos esperamos que no lo sean, pero desde luego nos han costado mucho todos y este no ha sido menos. Como de costumbre, ya casi una tradicion, este numero llega tarde... pero llega, y cargado de nuevos textos y colaboradores, que poco a poco nos van liberando de tareas que nuestras ocupadas vidas profesionales actualmente no nos permiten realizar.

Este es desde luego un numero de transicion por muchas razones, como todo en la vida, SET tambien esta cambiando, no se si para mejor o para peor, y son muchas las razones que nos llevan a ello, pero sobre todo una: cada dia somos mas viejos!. Pero los fundamentos que originaron este e-zine siguen en pie por mucho que cambien las maneras y las formas.

Seguimos realmente convencidos de nuestro proyecto, el proyecto de conocer, el proyecto crear y como no, el de destruir...

Volviendo al tema inicial, este es un numero de transicion tambien por razones ajenas a nuestra voluntad, estais leyendo estas lineas, la LSSI ya esta en vigor. A los miembros de SET nunca se nos dieron muy bien las leyes, y asi bote pronto, desconocemos cuales seran las consecuencias de dicha ley, eso nos lo dira el tiempo, y por supuesto, vosotros.

Otras razones por las que este es un numero de transicion, por que este numero carece de editor. Aunque este articulo esta firmado por editor, en esta ocasion y muy posiblemente de ahora en adelante, todo el staff de SET sera editor, liberando muchas labores que llevaba a cabo el editor.

Esperamos que de esta manera los editores no se nos "mueran" jovenes.

Lo ultimo que os quiero comentar es que si os fijais en este numero tamien se ha caido una seccion que ya era un clasico de nuestros numeros el SET inbox, no os precupeis en futuros numeros volvera a aparecer, tambien los mas observadores vereis que la interfaz de SET comienza a "mutar" poco a poco, y esto es porque en sucesivos numeros intentaremos minimizar el ASCII que a la hora de la verdad nos trae mucho trabajo.

Tal y como decia un antiguo editor de SET:

Pase lo que pase, tener cuidado ahi fuera.

EOF

-[0x02]----------
-[Crack de una Hyena]----------
-[by madfran]----------SET-26-

COMO LOGRAR UNA HERRAMIENTA MULTITAREA

INTRODUCCION

A veces nos encontramos con el problema de querer saber cual es la direccion IP de una maquina de la cual solo sabemos o intuimos su nombre. A menudo queremos ver que servicios dispensa un servidor. De vez en cuando nos interesa saber que servidores se encuentran en nuestra red. Estamos suponiendo que nos encontramos dentro de una red muy grande y que en ella se inpone el dominio del todopoderoso Windows. Que mejor herramienta que una hyena!. No pretendemos hablar sobre un mamifero que habita en las lejanas (para nosotros) sabanas africanas. Nos estamos refiriendo a una magnifica herramienta llamada Hyena, que va por la version 4.2 'C' y que ha sido desarrollada por una empresa llamada SystemTools Software Inc.

UN DESEO INCONTROLADO

Es el que te corroe cuando te encuentras dentro de una red que por alguna razon intuyes es enorme pero que desconoces casi por completo. Cuales son las razones por las cuales te puedes encontrar ante semejante comezon?, pues,... infinitas como las situaciones que se encuentran en la vida real.
Tal vez eres un consultor al que han dado un acceso a la red, pero el acceso es provisional y tremendamente recortado, bueno solo para hacer un trabajito miserable. A lo mejor eres un estudiante mal pagado y peor tratado, provisto de contrato para hacer un estudio de verano de esos que si son buenos, acostumbran a ser fagocitados por algun caza medallas de la empresa que te chupa la sangre. Como ya os hemos dicho puede ser variadas la situaciones y los motivos pero la consecuencia siempre es la misma, cuando te encuentras con la cabeza hecha un torbellino y necesitas descansar hay varias soluciones, ir al lavabo, buscar una maquina de cafe, molestar al vecino, intentar ligar con la persona del mismo u opuesto sexo que se encuentre en las proximidades o... rastrear a ver que basura encuentras en la red de marras.

Es el momento de lanzar el programita Hyena!. No es que sea la panacea universal pero te da un vistazo de todo el entorno de tu ordenador. Y entonces, ahi vamos! nos lanzamos a ver que pasa. De repente,... la desilusion!. El problema es que en lugar de darte la informacion deseada, te larga un mensajito diciendo que han pasado los treinta dias de evaluacion y si no sabes el codigo correcto no hay nada que hacer. En este momento nos acordamos que el programita en cuestion hace una porrada de dias que lo habiamos usado y que la licencia de treinta dias, hacia tiempo que habia expirado.

NO NOS DAMOS POR VENCIDOS

Eso nunca! Se pueden tardar dias, meses o anyos pero lo principal es nunca darse por vencido! Es la base de cualquier estrategia para evitar quedarnos a las puertas de la fiesta... y a nosotros no nos gusta que nos den con la puerta en las narices (duele en las narices y en el amor propio).

Hay que empezar por decidir cual es la mejor estrategia a seguir y hay varias a nuestra disposicion. La mas sencilla es intentar que otro haga el trabajo sucio por nuestro cuenta o sea buscar un cracker en la red. En teoria basta con utilizar www.google.com, buscar hyena y... comprobar que te aparecen algunas miles de refencias. Buf! Que aburrido! vamos a hacernos el trabajo nosotros mismos!

Si no nos gusta que otro hago el trabajo que unicamente es de nuestra competencia, tenemos que seguir los tipicos pasos que cualquier buen cracker debe seguir:

- Buscar un desensamblador (en los sitios acostumbrados)
- Lanzarlo para desensamblar el programa objetivo (cuidando que no se escape)
- Fijarnos en algunos detalles pertinentes (los impertinentes, podeis obviarlos)
- Tomar nota de lo que hay que cambiar (en papel u objeto similar, no os fieis de vuestra, deplorable, memoria)
- Buscar un editor hexadecimal (en el mismo sitio que antes)
- Realizar con el, los cambios deseados (... ni uno mas ni uno menos)
- Comprobar que todo marcha segun tus deseos (que no tienen que coincidir con los deseos del fabricate del software objetivo)

EL DESEMSAMBLADOR

El otro dia recibi una consulta de una persona perdida en internet, que me preguntaba para que servia un desensamblador (veridico y cierto, si no os lo creeis os puede ensenyar el e-mail), dado que desconozco el grado de conocimiento (o de desconocimiento) de mis atentos lectores (hay alguien despierto?), paso a hacer una breve descripcion... Un desensambblador, no es nada mas que un programita que convierte un galimaties de cifras y numeros, en codigo en assembler. Si el programita es lo suficientemente bueno, ademas del codigo puro y duro, os obsequiara tambien con algunas descripciones, y el texto de todos los menus y comentarios que el programa a crackear te vomita de vez en cuando.

Perfecto! Ahora pasemos a la busqueda de un software de este estilo. Todo un clasico en la materia es el famosisimo W32Dasm. Hay diversas versiones, todas funcionan correctamente pero son de pago, o sea la version que podeis encontrar esta limitada en algunos sentidos, pero basta para nuestros deseos. El productor de esta maravilla es la empresa URSoftware Co. que se ganaba la vida haciendo diversas cosas pero parece que no le ha ido nada bien ya que ha desaparecido del mapa. Si no os gusta o no lo encontrais, una buena alternativa es el IDA, pero yo me desenvuelvo tranquilamente con la version 8.7 del W32Dasm aunque se que existen versiones posteriores hasta la 8.93.

DESENSAMBLANDO

En fin, una vez encontrais lo que os hace falta solo hay que lanzar el programa y a continuacion desensamblar el Hyena. En codigo ASCI genera un monstruo de mas de 18 Mb y buscar a pelo por ahi dentro no es tarea para realizar de buenas a primeras. Hay que actuar, sino con metodo, como minimo con un poco de inspiracion. Lancemos el Hyena y fijemonos en que nos dice. Ademas de comunicarnos el sistema de registro, nos dice los dias que quedan para disfrutar de la licencia provisional (exactamente cero dias) con el siguiente mensaje

"Days remaining in trial period"

Lo mas evidente es buscar en el codigo desemsamblado el texto en cuestion. No lo encontramos en el cuerpo del codigo, pero si encontramos este dialogo.

```
Name: DialogID_0099, # of Controls=012, Caption:"Registration"
     001 - ControlID:FFFF, Control Class:"" Control Text:""
     002 - ControlID:FFFF, Control Class:"" Control Text:"This is a fully
           functional copy of Hyena.  Registration is required after the "
     003 - ControlID:0638, Control Class:"" Control Text:"http://www.systemtools
           .com/hyena"
```

```
     004 - ControlID:FFFF, Control Class:"" Control Text:"If you have your
           registration information for Hyena, enter it below, and then "
     005 - ControlID:FFFF, Control Class:"" Control Text:"Days remaining in
           trial period"
     006 - ControlID:0458, Control Class:"" Control Text:""
     007 - ControlID:FFFF, Control Class:"" Control Text:"Registration Key"
     008 - ControlID:0459, Control Class:"" Control Text:""
     009 - ControlID:FFFF, Control Class:"" Control Text:"Company / Licensee
           Name"
     010 - ControlID:0488, Control Class:"" Control Text:""
     011 - ControlID:0002, Control Class:"" Control Text:"&Registration
           Infomation"
     012 - ControlID:5190001, Control Class:"" Control Text:"OK"
```

Hacemos otro intento, buscando el DialogID-0099 pero encontramos demasiadas referencias sin ninguna que diga nada sobre Controls_ID=012..... parece que nos encontramos en un punto muerto !

BUSCANDO CON UN POCO MAS DE PACIENCIA

Cuando ponemos el codigo equivocado de registro, el programa nos entretiene con un obsceno (cada cual tiene su propio concepto de la obscenidad) mensaje

"The trial period has expired"

Normalmente, cuando recibes un mensaje semejante, el danyo ya esta hecho y el programa no funciona, pero... y si este no es el caso?

Ni cortos ni perezosos nos lanzamos a la busqueda del presunto tesoro y encontramos este pedazo de codigo.

```
************************************************************************
********* UN PEAZO DE CODIGO ***********************************************
************************************************************************


:004332B9 E810820800              Call 004BB4CE
:004332BE 8D4C241C                lea ecx, [esp + 1C]
:004332C2 C7842450070000FFFFFFFF  mov dword ptr [esp + 00000750], FFFFFFFF

* Reference To: MFC42u.MFC42u:NoName0122, Ord:0320h
                                  |
:004332CD E8FC810800              Call 004BB4CE
:004332D2 B801000000              mov eax, 00000001
:004332D7 E9EE040000              jmp 004337CA

* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:
|:00432E15(C), :00432E27(C), :00432E78(C), :00432EF4(C), :00432F06(C),
|:00432F3C(C)
|
:004332DC 85FF                    test edi, edi
:004332DE 0F858A020000            jne 0043356E
:004332E4 6A10                    push 00000010

* Reference To: USER32.MessageBeep, Ord:01C2h
                                  |
:004332E6 FF15F86A4D00            Call dword ptr [004D6AF8]
:004332EC 6AFF                    push FFFFFFFF
:004332EE 6A10                    push 00000010

* Possible Reference to String Resource ID=21343: "The trial period has expired.  "
```

```
                                   |
:004332F0 685F530000               push 0000535F

* Reference To: MFC42u.MFC42u:NoName0187, Ord:04ACh
                                   |
:004332F5 E848830800               Call 004BB642


*****************************************************************************
********* OTRO PEAZO DE CODIGO ***********************************************
*****************************************************************************

* Reference To: MFC42u.MFC42u:NoName0246, Ord:048Dh
                                   |
:00433868 E8317F0800               Call 004BB79E
:0043386D 8BBC2414020000           mov edi, [esp + 00000214]
:00433874 8B7004                   mov esi, [eax+04]
:00433877 6A00                     push 00000000
:00433879 57                       push edi

* Possible StringData Ref from Data Obj ->"C"
                                   |
:0043387A 68A0515000               push 005051A0
:0043387F 8BCE                     mov ecx, esi

* Reference To: MFC42u.MFC42u:NoName0249, Ord:0DBCh
                                   |
:00433881 E82A7F0800               Call 004BB7B0
:00433886 85C0                     test eax, eax
:00433888 7423                     je 004338AD
:0043388A 6A10                     push 00000010

* Reference To: USER32.MessageBeep, Ord:01C2h
                                   |
:0043388C FF15F86A4D00             Call dword ptr [004D6AF8]
:00433892 6AFF                     push FFFFFFFF
:00433894 6A10                     push 00000010

* Possible Reference to String Resource ID=21343: "The trial period has expired.  "
                                   |
:00433896 685F530000               push 0000535F

* Reference To: MFC42u.MFC42u:NoName0187, Ord:04ACh
                                   |
:0043389B E8A27D0800               Call 004BB642
:004338A0 5F                       pop edi
:004338A1 33C0                     xor eax, eax
:004338A3 5E                       pop esi
:004338A4 81C408020000             add esp, 00000208
:004338AA C20400                   ret 0004

*****************************************************************************
*****************  FIN DE ROLLOS DE CODIGO **********************************
*****************************************************************************
```

Vosotros podeis hacer lo que querais, pero yo os aconsejo que no hagais caso del segundo trozo de codigo y os centreis en el primero. Para ser mas precisos en el codigo que pone,

```
85FF
0F858A020000
6A10
```

Y lo cambiais por un,

```
85FF
0F848A020000
6A10
```

(diablos! fijaros bien! he cambiado un 5 por un 4)
Con esto un jne se reconvierte en un je (Para los que os hallais dormido esto quiere decir antes saltaba "si no es igual" y ahora solo salta "si es igual") y solo te sale el malefico mensaje si por casualidad aciertas el codigo de registro (que tambien seria mala suerte!)

TRABAJANDO CON UN EDITOR HEXADECIMAL

Hasta ahora solo hemos trabajado con la mente (que es cosa sabia, pero siempre se termina bajando de las nubes) pero un dia u otro hay que pisar tierra firme y empezar a ensuciarse las manos,.... o sea hay que realizar fisicamente el trabajo de la modificacion del codigo.

Para ello se requiere un editor hexadecimal. Existen millones en la red y muchos con parafernalia de dibujitos e incluso musiquitas, pero yo prefiero un editor pelao de toda la vida que no ocupa casi nada y es viejo como la tos pero no da sorpresa ninguna. Me refiero al PSEDIT, venerable herramienta donde las haya (creo que data de 1994) que todavia reclama un registro de 24 dolares y que pagaria a gusto si su creador no hubiera desaparecido de toda referencia conocida en el mundo civilizado.

Con dicho editor, y una vez pasado los reclamos de pagos atrasados, se abre el archivo hyena.exe Los que llegeis ahi solo vereis una lista de datos rarisimos os adjunto un poco para que os hagais una idea.

```
00000020  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   ................
00000030  00 00 00 00 00 00 00 00-00 00 00 00 18 01 00 00   ................
00000040  0E 1F BA 0E 00 B4 09 CD-21 B8 01 4C CD 21 54 68   ........!..L.!Th
00000050  69 73 20 70 72 6F 67 72-61 6D 20 63 61 6E 6E 6F   is program canno
00000060  74 20 62 65 20 72 75 6E-20 69 6E 20 44 4F 53 20   t be run in DOS
00000070  6D 6F 64 65 2E 0D 0D 0A-24 00 00 00 00 00 00 00   mode....$.......
00000080  AB 7E 0F 59 EF 1F 61 0A-EF 1F 61 0A EF 1F 61 0A   .~.Y..a...a...a.
00000090  07 00 65 0A ED 1F 61 0A-B9 00 72 0A E7 1F 61 0A   ..e...a...r...a.
000000A0  B2 3D 6A 0A EC 1F 61 0A-6C 03 6F 0A EA 1F 61 0A   .=j...a.l.o...a.
000000B0  B2 3D 6B 0A E4 1F 61 0A-B2 3D 65 0A ED 1F 61 0A   .=k...a..=e...a.
000000C0  96 3E 6A 0A EC 1F 61 0A-96 3E 65 0A ED 1F 61 0A   .>j...a..>e...a.
000000D0  07 00 6A 0A EC 1F 61 0A-EF 1F 61 0A E3 1F 61 0A   ..j...a...a...a.
000000E0  B6 3C 72 0A FC 1F 61 0A-EF 1F 60 0A B1 1C 61 0A   .<r...a...‘...a.
000000F0  B0 3D 6A 0A CF 1F 61 0A-28 19 67 0A EE 1F 61 0A   .=j...a.(.g...a.
00000100  52 69 63 68 EF 1F 61 0A-00 00 00 00 00 00 00 00   Rich..a.........
00000110  00 00 00 00 00 00 00 00-50 45 00 00 4C 01 04 00   ........PE..L...
00000120  6B 40 0A 3D 00 00 00 00-00 00 00 00 E0 00 0F 01   k@.=............
00000130  0B 01 06 00 00 50 0D 00-00 30 08 00 00 00 00 00   .....P...0......
```

La parte izquierda es el indice del archivo (16 en hexadecimal es igual a 10), en el centro esta el verdadero programa en codigo maquina y a la derecha esta una traduccion literal en codigo ASCII, que solo sirve para algo cuando se encuentra dentro del codigo algun texto para humanos ojos.

Como hemos dicho antes, se trata de buscar un trazo de codigo igual a

```
85FF
0F858A020000
6A10
```

Por lo tanto con el buscador del propio editor os divertis a buscar la secuencia
85FF0F858A0200006A10
Aseguraros Que solo hay una, porque sino podeis cambiar cualquier cosa menos lo que deseais. Una vez encontrada, no hay nada como cambiarla por

85FF
0F848A020000
6A10

despues lo salvais y listo.

COMPROBANDO QUE TODO FUNCIONE CORRECTAMENTE

Pues es tan sencillo como substituir el hyena.exe de origen por vuestra copia manipulada. Lo lanzais y comprobais los resultados

ALGUNOS COMENTARIOS FINALES

Tal vez os preguntareis que encontre en la red origen de todos estos trabajos. Pues tampoco cosas del otro mundo. Como es moneda corriente, un monton de servidores semiabandonados, muchas impresoras, servidores de CD, algunas trazadoras, incluso algunos servidores convenientemente mantenidos, pero sobretodo,... cientos de PCs ociosos o rellenos de la mas estrambotica busura.

Curiosidades de la vida. Si en vez de utilizar el W32DASM, utilizais el OllYDBG (otro dia escribire sobre el), se puede ver que el programita HYENA esta prelicenciado a AMERITECH-SBC. Si alguno de los lectores sabe por que y como esta registrado, please, me lo comunique. Tengo mucha curiosidad, (me parece que es de lo unico que tengo en abundancia) pero ya sabeis que no tengo tiempo ni conocimientos suficientes para aranyar en el interior de programas ajenos.

EOF

```
-[ 0x03 ]--------------------------------------------------------------------
-[ Bazar]--------------------------------------------------------------------
-[ by diversos autores ]-----------------------------------------------SET-26--

Que es eso? es un barco? es un avion? es un articulo? NO!!!
ES EL BAZAR DE SET!!!

Otro numero mas damos la oportunidad de publicar en SET a gente que
no se ve con animos para escribir penyazos tan largos como los que
suelen ir sueltos o quieren enviarnos sus trucos, opiniones o pequenyos
descubrimientos.

Como de costumbre, si deseais escribir, los articulos los enviais
a <set-fw@bigfoot.com> o a setup.rul
nos da un fichero bastante largo.

Ejecutamos el instalador, metiendo un numero cualquiera, y da el error
"You have entered an invalid product code.  Click OK and try again."
Asi que buscamos esta cadena en el fichero:

SprintfBox(-65533, "Invalid Product Code", "You have entered an invalid
product code.  Click OK and try again.");

Vamos bien.
Esa linea se encuentra en la funcion
function118()
que es llamada desde varios sitios.
Sin mas que echar una ojeada al trozo de codigo:
function119()
00378C:002F:         StrLength(string18);
003791:0021:         lNumber3 = LAST_RESULT;
003799:0128:         lNumber3 = lNumber3 != 31;
0037AB:0022:         if (lNumber3 = 0) then
                         goto label134;
                     endif;
0037B9:00B5:         function118();
0037C1:012F:         return(1);
......

O sea: si StrLength(string18) no vale 31, el codigo no vale.
Pues eso, que el codigo debe contener 31 caracteres.
Seguimos mirando hacia arriba, hasta ver donde se inicializa string18
........
0014A6:0013:         string18 = "fffffffffffffffffffffffffff7";
y tambien
00707B:015E:         SilentWriteData(string1, "szEdit1", 1, lString4, 0);
007097:015E:         SilentWriteData(string1, "szEdit2", 1, lString5, 0);
0070B3:015E:         SilentWriteData(string1, "szEdit3", 1, lString6, 0);
0070CF:015E:         SilentWriteData(string1, "szEdit4", 1, lString7, 0);
0070EB:015E:         SilentWriteData(string1, "szEdit5", 1, lString8, 0);
007107:015E:         SilentWriteData(string1, "Result", 2, "", lNumber0);
007120:0124:         lString10 = lString4 + lString5;
00712B:0124:         lString10 = lString10 + lString6;
007136:0124:         lString10 = lString10 + lString7;
007141:0124:         string18 = lString10 + lString8;
........
Esto es, se toman de una ventana de dialogo que tiene 5 TextBox

Un poco mas:
0013FD:0125:         lString3 = SUPPORTDIR ^ "SampleDLL.dll";
001415:00B2:         UseDLL(lString3);
00141A:0021:         lNumber0 = LAST_RESULT;
```

```
001422:0013:         string21 = string18;
00142A:0013:         lString2 = "                                ";
001451:00B4:         SampleDLL.CompareLicense(string21, lString2);
00145C:0021:         lNumber0 = LAST_RESULT;
001464:0023:         StrCompare(lString2, "Boooooo");
001473:0128:         lNumber2 = LAST_RESULT = 0;
001485:0022:         if (lNumber2 = 0) then
                         goto label24;
                     endif;
```

Vaya, asi que se carga SampleDLL.dll que tambien se crea temporalmente
cuando arrancamos el instalador.
Luego se llama a la funcion CompareLicense con string21 (=string18)
Lo mas curioso es que el resultado de esta funcion se vuelve a guardar
en lString2, asi que es un parametro de entrada y salida.
Ademas, luego se compara si lString2 vale "Boooooo". Pues ya nos podemos
imaginar lo que va a pasar: que la clave es incorrecta.

Asi que ya lo tenemos todo:

-Podemos parchear SampleDLL.dll para que nunca devuelva "Boooooo"
 Pero SampleDLL.dll se descomprime al iniciar el instalador, asi que no
 la podemos modificar previamente. Mala suerte.

-Podemos modificar el fuente setup.rul para que no ejecute ese trozo de
 codigo, pero eso obligaria a recompilarlo, y habria que tener la
 version de InstallShield que permite recompilar, que tampoco tenemos.

-Podemos parchear setup.ins donde dice "Boooooo" para que diga "Bien"
 Asi la comparacion con "Boooooo" nunca tendra exito; es decir, el validador
 de claves siempre dira que la clave esta bien.

Dicho y hecho. Tomar un editor hexadecimal, buscar "Boooooo", y cambiarlo.
Ya podemos usar cualquier clave (de 31 digitos)

Segunda parte.

No todo podia ser tan bonito.
Cuando intentamos instalarlo, la lista de subproductos instalables se reduce
a solo 1 subproducto, pero sabemos que hay mas.
Lo que pasa es que la clave tambien contiene los subproductos para los que
has adquirido licencia. El paso anterior solo vale para que pase la prueba
del checksum :-(

Investigando un poco mas descubrimos este trozo de codigo:

```
003A93:007A:         GetByte(lNumber3, string18, 30);
003AA0:011A:         lNumber3 = lNumber3 - 97;
003AAD:0119:         number41 = lNumber3 + 10;

label141: //Ref: 003A8A
003AC4:0128:         lNumber3 = number41 = 2;
003AD6:0022:         if (lNumber3 = 0) then
                         goto label143;
                     endif;
003AE4:0013:         string11 = "ora";
003AEF:0013:         string12 = "ORACLE";
.....
label143: //Ref: 003AD6
003B14:0128:         lNumber3 = number41 = 3;
003B26:0022:         if (lNumber3 = 0) then
                         goto label144;
```

```
                    endif;
003B34:0013:        string11 = "inf";
003B3F:0013:        string12 = "INFORMIX";
......
label144: //Ref: 003B26
003B68:0128:        lNumber3 = number41 = 4;
003B7A:0022:        if (lNumber3 = 0) then
                        goto label145;
                    endif;
003B88:0013:        string11 = "dbx";
003B93:0013:        string12 = "DB2UNIX";
......
label146: //Ref: 003BCD
003C0B:0128:        lNumber3 = number41 = 7;
003C1D:0022:        if (lNumber3 = 0) then
                        goto label147;
                    endif;
003C2B:0013:        string11 = "mss";
003C36:0013:        string12 = "MICROSFT";
```

O sea, que se obtiene el caracter 30-esimo de string18, se le quita 97 (caracter 'a'), se suma 10, y se compara con "2" y si es cierto, string12 = "ORACLE"
Si no, se compara con "3" y si es cierto, string12 = "INFORMIX";
En resumen, el caracter 30 debe transformarse en 2 para ORACLE, 3 para INFORMIX,
4 para DB2UNIX, y 7 para MICROSFT (SQL Server)
Volviendo hacia atras, si el caracter 30 es 'Y', su valor es 89; se le resta 97, se le suma 10, quedando 89-97+10=2, y se instala sobre ORACLE.

Asi que ya podemos instalarlo en cualquier base de datos.

Da gusto que con solo 1 CD se puedan instalar todos los productos sin mas que tener la clave adecuada.

Y esto es todo. Necesite 5 minutos para saber que tenia que atacar al instalador, 30 para encontrar un descompilador, 10 para entender el codigo, 10 para parchearlo, y 4 horas para instalarlo en ORACLE. Pero ya he dicho antes que el producto cuesta varios miles de dolares, e incluye funcionalidad que solo usan grandes, muy grandes empresas.

FCA00000

****
[3x02] Que son los hexadecimales por Jepkc
****

Hola amigos de SET soy Jepkc, es la primera vez que escribo un articulo para esta y cualquier otra e-zine.

Veran, lo de los hexadecimales es sencillo.

Para el pueblo mas neofito explicare, los hexadecimales son otro sistema numerico por ejemplo:

```
-----------------------------
Sistema
-----------------------------
Decimal         Hexadecimal
0               0
1               1
```

2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F

Ahora viene la parte interesante.
Cuando se compila un programa en cualquier tipo de Sistema (Hasta los gameboy) se guarda en hexa los diferentes valores por ejemplo la letra A puede ser A2 que es un hexadecimal.

Al querer traducir un programa se necesitan:

Requerimientos Minimos:

-Una computadora
-Un teclado
-Translhextion (creo que lo he escrito mal)
-El THINGY hecho por un tio que se llama NecroSacro.
-Un mogollon de tiempo libre

Primero consiguete el THINGY, no te consigas el codigo en BAS (Si escucharon bien esta hecho en Basic) porque te llena la pila de porquerias, mejor consiguete el ejecutable ya compilado. Hay una version para 32 bits (windows) pero es la misma vaina.

Segundo debes conseguir un programa que se llama Translhextion que te va a hacer las tablas. No sabes que son las tablas? ... ha cierto no lo he dicho ! te acuerdas que arriba decia que la letra A podia se A2 ?, bueno las tablas lo que hacen es eso, o sea el trabajo sucio, el Translhextion mediante un metodo que se llama Busqueda relativa (Relative Search) busca palabras por el metodo relativo (valga la redundancia). Se trata mas o menos de buscar asignando un valor a la primera letra es decir, aqui un ejemplo.

Letra	Hexa
A	A1
B	A2
C	A3
.	.
.	.
.	.

(Mas abajo siguen la demas letras, las minusculas y un mogollon de simbolitos como ?=, etc)

Es decir a partir de la letra A se comienza a sumar 1 a los signos siguientes.

Si estas traduciendo una ROM entonces debes entrar a la ROM y buscar una palabra grande por ejemplo, si durante el juego un personaje dice:"Jepkc es un atorrante" y tu crees que eso es mentira entonces debes anotar la palabra "Atorrante" (case sensitive) luego ir al Translhextion y entrar a Relative

Search (buscalo, esta por los menus) te sale un Cuadro de Dialogo y ahi debes escribir la palabra "Atorrante"... y esperar bastante (al menos si es que estas trabajando en una 486... os aseguramos que estas maquinas existen y funcionan egregiamente) te va a arrojar los resultados y despues preguntara si es que deseas hacer una Tabla (me imagino que ya tienes claro que es una tabla).

Guardas esta tabla en el directorio del THINGY (es una recomendacion) y luego abres el THINGY le indicas el nombre de la table por ejemplo: tablita.tbl y luego el nombre del archivo por ejemplo: mentira.gbc y presionas S o B depende si tienes la version en Espanyol o en Ingles el THINGY te va a preguntar que deseas buscar, entonces debes poner la frase:"Jepkc es un atorrante", luego el programa te lleva a el lugar donde esta el error y cambias la frase por algo diferente que puede ser cualquier cosa siempre y cuando tenga la misma longitud de caracteres, por ejemplo:

```
Frase vieja: Jepkc es un atorrante
Frase nueva: Jepkc es un hacker 31337           /*
Esta frase es muy grande
Frase nueva: Jepkc es tan 31337...              /*
Esta es casi perfecta
```

Como podeis ver, cabe exactamente pero quedan 3 espacios en blanco. El mecanismo
es el mismo tanto con una Rom que con un programa de Guindows creo que hasta podria funcionar con una Mac.

Quiza en algun proximo texto esplicare como funciona el Resource Workshop.

Cualquier duda, problema, error, etc pueden enviarla a jepkc@yahoo.com
Los flames se pueden mandar a las operadoras de telefonica numero 123

****

[3x03] Consola Philips by Groovy

****

Algunos Bugs en las consolas Phillips de SKY en Argentina.

Primer Bug:
Este bug se puede reproducir al apretar un boton de un canal no existente, por ejemplo el "3", y antes de que envie la señal para ir al canal noexistente apretar alguno de los botones de volumen "+" o "-" y comprobaras asombrado que la barra que te indicaba el estado del volumen no esta mas.

Segundo Bug:
Este bug sirve para sacar por unos segundos la molesta pantalla que te dice que compres la pelicula. Este cartelito es bastante molesto cuando la pelicula es subtitulada, porque el cartel justo tapa los subtitulos no dejandote leerlos y por lo tanto saber como empieza la pelicula.
Para sacarlo apretar el boton "+" o plus (o el que hace aparecer el menu para cambier de idioma) dos veces consecutivas, y el menu desaparecera por unos 40 segundos.
Si te aparece de vuelta podes volver a apretar la misma conbinacion. (logico no ?)

Como acceder a los menus de programacion de la consola?
Si el que te puso la consola en tu casa es medio bolu... te aseguro que el codigo de acceso a todos los menues va a ser "0"0000 (el cero entre comillas es

el que ya esta puesto).

Bueno espero que los encuentren de su agrado y voy a tratar de descubrir mas bugs para este sistema.
COPYRIGTHS DE LOS BUGS A GR00VY
Alguna sugerencia a groovy2600@yahoo.com.ar

```
*****************************************************************************
[3x04] Crack salvapantallas                              by Mago
*****************************************************************************
```

```
       ------------------------------------------------------------
       Explicacion sobre la sencilla forma de romper el algoritmo del
       salvapantallas de windows.
       ------------------------------------------------------------

                          (Realizado por [MaGo])
```

Este texto tratara de, tal y como dice su titulo, explicar en que consiste la encriptacion del password del salvapantallas de Windows, y como "crackearlo manualmente", ya que, es demasiado facil. Tal vez, este texto algunos lo consideren una tonteria, pero lo considero algo mas o menos interesante. Que porque escribi este texto? Bueno, la verdad es que hablando sobre este tema, creo o que no hay nada en espanyol, o poco se ha escrito de ello. Encontre un extenso articulo en ingles en http://hackingtruths.box.sk/screen.htm que trataba este tema, y decidi ponerme manos a la obra. Antes de nada decir que utiliza lo que se llama encriptacion XOR (operacion logica ;)), asi que mis debidos respetos a los que ya sepan que es, pero me veo obligado a explicarlo ok?

Lo que se conoce como XOR es una operacion logica, bastante utilizada en virus y en diversos programas para protegerlos de "crackers".
(Decir que XOR quiere decir eXclusive OR)
Es bastante sencillo, os comento:

Valor + llave = valor encriptado.

Valor encriptado + llave = Valor original.

Cojemos dos valores binarios, a partir de ahora seran valor a encriptar y llave.
Por ejemplo:

```
      4Fh en binario >> 01001111 (Valor a encriptar)
      D1h en binario >> 11010001 (Llave con la que se encripta)
                        --------
                        ???????? (Aqui iria ya el valor encriptado)
```

Bien, como hace la operacion? Pues si un bit del valor es igual que el de la llave, da como resultado 0 y sin son distintos 1. Asi que seria:

```
      4Fh en binario >> 01001111 (Valor a encriptar)
      D1h en binario >> 11010001 (Llave con la que se encripta)
                        --------
                        10011110 (Valor encriptado, 9Eh)
```

Para obtener el valor original, o lo que es lo mismo, desencriptarlo, debemos conocer la llave (Mirar mas arriba para ver la operacion).

```
      9Eh en binario >> 10011110 (Valor encriptado)
      D1h en binario >> 11010001 (Llave)
```

```
                        --------
                        01001111 (Valor original!! 4Fh)
```

Esta es la operacion XOR base, de llave de 8 bits, pero las llaves pueden ser de mas bits, anyadiendole mas seguridad a la encriptacion. Pero nosotros solo nos interesa la de 8 bits, ya que es la que utiliza el password del salvapantallas. (Microsoft, aparte de muchas cosas, tiene fama de la debil seguridad de sus sistemas :-P)

Bueno, una vez explicado lo de XOR, vamos con el password de la contrasenya de windows.
Lo primero que hay que saber, donde se localiza?
En los Windows 3.x se localizaba en el fichero control.ini en la carpeta de windows.
En los Windows 9x y posteriores, se localiza en el registro de windows en la clave
HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSave_Data
o lo que es lo mismo, como el registro de windows se almacena en dos archivos, user.dat y system.dat, si buscamos con cualquier editor de textos (menos msword y notepad) la palabra "ScreenSave_Data"a continuacion encontrariamos la password.

Bien, ahora recomendaria una herramienta para convertir de hexadecimal, a binario, a ascii etc. Una muy buena herramienta bajo windows es STC y la podeis encontrar en la direccion http://www.kryptocrew.de/snakebyte/

Muy bien, vamos a coger por ejemplo la palabra "DOME" y la vamos a introducir como contrasenya del salvapantallas. Si miramos el user.dat, la palabra DOME corresponde con 0CA13B58.

Por lo tanto, cada cifra de la palabra DOME corresponde con dos del password encriptado, D = 0C O = A1 M = 3B E = 58.
Si D es 44 en hexadecimal, 0 es el primer 4 encriptado y C es el segundo 4 encriptado. Si conocemos los valores originales y los encriptados, como podemos obtener la llave?

Pues facil, debemos de procurar que la operacion XOR se cumpla:

```
      0 en binario >> 00000000 (Valor encriptado)
                      ???????? (Llave)
                      --------
                      00000100 (Valor original, 4)
```

Si queremos que la operacion XOR se cumpla, debemos de fijarnos que para que el 0 del valor encriptado de 0 en el valor original, deberia de haber otro 0 en la llave, asi consecutivamente obtenemos la primera llave:

```
      0 en binario >> 00000000 (Valor encriptado)
                      00000100 (Llave)
                      --------
                      00000100 (Valor original, 4)
```

Decir que la contrasenya solo puede contener 14 caracteres, y que si por cada caracter hay dos valores encriptados, en total solo puede haber 28 llaves. En el texto original venia al final todas las llaves de cada valor, asi que tambien lo voy a incluir en este texto al final.

Vamos con el valor C:

```
      C en binario >> 00001100 (Valor encriptado)
                      00001000 (Llave, mirar al final del texto)
                      --------
```

```
                    00000100 (Valor original, 4)
```

Por lo tanto, hemos obtenido el valor 44h, que en ascii corresponde con la letra
D!!!!!!! Tenemos la primera letra!!!
Ahora vamos a ver lo mismo, pero con una clave diferente, por ejemplo ERIKA que corresponde con 0DBC3F5626.

```
      0 en binario >> 00000000 (Valor encriptado)
                      00001000 (Primera llave, mirar al final del texto)
                      --------
                      00000100 (Valor original, 4)

      D en binario >> 00001101 (Valor encriptado)
                      00001000 (Segunda llave)
                      --------
                      00000101  (Valor original, 5)
```

Asi obtenemos el valor 45h que corresponde con la letra E!!!
Si hicieramos los mismo con cada una de las letras de la password y con las llaves que incluyo al final del texto, podeis desencriptar cualquier password que querais!!

Pero...que finalidad tiene este texto? Bueno, en realidad la finalidad la dejo en manos vuestras, es solo cuestion de pensar un poco, por ejemplo para conseguir la contrasenya remotamente hacer un programa que al ejecutarlo la "victima" coja el password y te lo envie por email, o simplemente imaginaos que esa persona utiliza la misma contrase~a para todo...
En fin, simplemente calentar un poco las neuronas ;)

A continuacion incluyo la tabla de las llaves:

	Primera llave de la clave encriptada	Segunda llave
1	00000100	00001000
2	00001110	00001110
3	00000111	00000110
4	00000001	00001101
5	00000110	00000111
6	00000110	00001001
7	00001010	00000001
8	00000001	00001011
9	00000111	00001010
10	00001000	00001100
11	00000100	00000111
12	00001111	00001000
13	00000101	00000100
14	00001001	00000101

Un saludo:

[MaGo]

```
*****************************************************************************
```

[3x05] Bug telefonia argentina by The crow root

```
*****************************************************************************
```

Este es un fallo que hemos descubierto desde hace ya un tiempo en uno de los servicios que ofrece Telefonica en la Republica de Argentina (no hemos sabido de otros paises, ya que el fallo se localiza en un servicio al cliente y no estamos seguros en que paises se brinda, pero aqui funciona perfectamente) y que ademas de funcionar perfectamente una vez advertido se sigue produciendo la

misma falla, es decir que la incompetencia que poseen estas personas para solucionar estos problemas le cuesta aproximadamente mas de $ 500.000 (aproximadamente $148.000 Dolares en 6 meses que es el tiempo que ha transcurrido desde que hemos descubierto el fallo, debido a la crisis que atraviesa Argentina damos la cantidad en Dolares) y esta cantidad de dinero es proporcional a la gente que utiliza este servicio que mas adelante se detalla, ya que a mayor cantidad de personas que lo utilizen con los propositos de no pagar llamadas mas dinero pierden, cabe destacar que la cifra antes mencionada se realizo a razon de 100 personas a una llamada por dia de 1 hora a costo internacional.

El servicio consiste en lo siguiente. En argentina se ha lanzado un nuevo servicio llamado "multiring" que consiste en que algun cliente X pueda acceder a un "segundo" numero sobre la misma linea fisica, es decir otro numero sobre el mismo aparato telefonico. No se trata de una segunda linea sino de un numero virtual. Este servicio en primer lugar se ideo para que lo utilizen personas que por X motivos posean el mismo numero telefonico para su hogar y para su trabajo. El servicio actua de esta manera, cuando se habilita les dan el "segundo" numero (virtual) entonces cuando llaman al numero virtual el timbrado del telefono cambia al del timbrado del numero habitual, es decir suponiendo que mi numero de TE es: 422222 (que lo usaria para llamdas de mi hogar) sonaria algo asi: Ring, Ring, Ring..., y una vez obtenido el segundo numero (421121 por ejemplo, que lo usaria para llamadas de trabajo) Este sonaria algo asi: Ring, Riiiiiiiiing, Ring, Riing... es decir que el timbrado seria un poco mas largo que el habitual, es por esto que dependiendo del timbrado se sabra de antemano que tipo de llamda seria, si es de trabajo o particular.

Bien ya hemos explicado el servicio ahora vayamos al fallo, como este segundo numero es "virtual" hemos descubierto que al realizar llamadas por cobro revertido a este segundo numero NO se facturan, inclusive si nuestra linea no se encuentra habilitada para recibir este tipo de llamadas con este numero si lo podra hacer, entonces podremos comunicarnos, siempre y cuando nos llamen a nosotros por cobro revertido, a cualquier parte del mundo y sin pagar ni un centavo, ni el que nos llama ni nosotros que recibimos la llamada. Esto esta comprobado y damos fe que funciona a la perfeccion.

Bueno, hemos explicado el fallo y como utilizarlo, ahora explicaremos algunos contratiempos que podemos tener: el primero es que al cabo de un tiempo este numero deja de recibir este tipo de llamadas, bien esto se soluciona perfectamente usando un poco de ingenieria social, llamamos al 112 que es el numero de atencion al cliente en mi pais y decimos por ejemplo que nuesto hijo les ha dado el numero virtual a sus amigos y que lo desearia cambiar ya que ese numero le habia dado un uso exclusivo para motivos de trabajo, o cualquier otra cosa o simplemente que me he cansado de que pregunten por X persona, ya que los "segundos numeros virtuales" NO son numeros nuevos sino que alguna vez han pertenecido a alguna otra persona que por X motivos ha decidido a dar de baja su linea telefonica.

Esto es todo por el momento y cualquier otra novedad les haremos saber,
cualquier consulta sobre este servicio o como utilizarlo,
mail a : The_Crow@hackers_rg.zzn.com
y resolveremos todas tus dudas.
Saludos a : Jhonny Bravo y muy especialmente a Any (Cba.).-

****
[3x06] Telefonica Spain by Portavoz
****

TELEFONICA, EL UNICO OPERADOR REAL

Ya he Hablado sobre los maravillosos servicios de Telefonica. Pero no es la unica companyia que nos oferta telefonia. Tenemos muchas otras. Han aparecido recientemente, y tambien nos echan mierda que debemos tragar. Y creer. Se supone que todas ellas son las mejores, que todas ellas son las mas utiles, las mas baratas y faciles de utilizar. Pero sabemos que no es asi. Estas companyias tambien abusan de nuestra confianza y el usuario medio esta completamente confundido ante la avalancha de tarifas que se nos vienen encima. Pero en ningun momento debemos olvidar a nuestro operador predilecto.

Soy consciente de que cuando Hablo, Hablo yo, y no el Espiritu Santo, pero alguien ha de Hablar, y ya que no lo hace ni el Espiritu Santo ni la "Television", me permito hacerlo yo.

El Gran Monopolio, a pesar de la liberalizacion nos sigue controlando. A nosotros y sus competidores, los cuales acaban pareciendo tener la culpa. Es de esto de lo que quiero Hablarles.

BT, Tele2, Uni2, Retevision, Telefonica, Alo, Airtel, y muchas otras cuyos nombres invaden nuestros cerebros diariamente. Desde la liberacion de las comunicaciones las nuevas companyias que ofrecen servicios telefonicos han surgido como setas. Pero lo mas curioso de todo esto es que todas ofrecen las mejores servicios, tarifas, precios. Unas ofrecen tarifas iguales a todas horas, otras descuentos impresionantes en llamadas a larga distancia, otros son mas baratos en las locales, otros en las interprovinciales. Pero ninguna dice toda la verdad.

Las que ofrecen tarifas iguales a todas horas son solo validas para las llamadas de larga distancia, las que tienen descuentos en estas son impagables a la hora de realizar llamadas locales, los que ofrecen rebajas en estas otras no sirven para llamar a telefonos moviles... Ninguna es la mas barata util. Que va ocurrir ahora? Y si nos damos de alta en todas estas companyias y las combinamos para pagar lo minimo en nuestra factura? Pues no, esto es inviable. Porque no es que nuestro telefono sea magico y se sepa todos los prefijos que inevitablemente tenemos que utilizar si queremos dirigir nuestra llamada por uno u otro operador. Si, claro, venden unos aparatitos muy majos que se llaman enrutadores. Pero cuanto cuestan? No mucho, ciertamente, a partir de unas 2000 pesetas, en dos meses de ahorrar telefono lo hemos pagado. Pero otro problema es que estos enrutadores tampoco son magicos y hay que programarle las tarifas. Y que vamos a hacer? Las tarifas cambian cada 2 meses, como quien no quiere la cosa. Y otro problema son las cuotas mensuales. No, no las hay, estaran pensando ustedes. Rete-uni-tele-airtel-vision les ha dicho que no hay cuota. Pero y nuestra queridisima Telefonica de Espanya S.A, que? Esta companyia SI cobra una cuota mensual. Bien, pues nos quitamos de Telefonica. NO! Telefonica y hasta el 2006 es duenya de las redes de comunicacion, asi que si queremos usar el cable que sale de nuestro bloque, chalet, o lo que sea, tenemos que tener a Telefonica contratada, y encima pagando un precio cada vez mas alto.

Bien, no voy a seguir explicando los muchisimos problemas a los que nos estan llevando todas estas companyias. Y no es que me oponga a la liberacion de las comunicaciones, todo lo contrario, pero ahora mismo esta liberacion no es efectiva. Como minimo no lo sera hasta el 2006 que podamos dar de baja nuestra linea con Telefonica y usar la de otros operador que no tendra que pagar precios desorbitados por los alquileres de la linea. Y lo mejor de todo es que para entonces habran quebrado mas de la mitad de estos operadores. Un ejemplo: Alo. Esta companyia ofrecia unos precios realmente apetitosas. La mitad de las tarifas que actualmente pagamos con Telefonica. Y es verdad. Era la unica companyia que ofrecia un buen precio en todas las llamadas. Pero lo que ocurre es que la barbara campanya de publicidad que han organizado no ha dado resultado. Y la razon es muy sencilla. La gran masa espanyola es muy cerrada, y no aceptamos esas innovaciones. Y claro, no han

obtenido los cientos de miles de clientes que esperaban y su filial en Espanya ha quebrado. Normal. Con todo esto no quiero decir que sigamos con nuestra Telefonica de toda la vida (Dios nos libre), ni que las demas sean peores, lo unico que pretendo es mostrar que la liberacion de las comunicaciones no es tal, y como minimo hasta que en el 2006 se produzca el reparto de las lineas no merecera la pena abonarse a ninguna otra companyia. Ademas, para esa epoca muchas de estas empresas habran quebrado. Las que no estan apoyadas por alguna poderosa companyia extranjera con capacidad para soportar las perdidas que actualmente tienen quebraran, y no todas. Vease Alo.

Por todo esto me gustaria insistir. Telefonica nos controla. Nos tiene bien sujetos a sus condiciones. No podemos plantarle cara. No podemos contratar otro operador para usarlo exclusivamente. Y Telefonica lo sabe. Y como lo sabe las tarifas de alquiler de la linea son cada vez mas altas. Porque saben que es lo unico que estamos obligados a pagarles.

Y todo esto lo hacen aprovechando que son el unico operador real que trabaja en Espanya: Telefonica, quien si no?

Portavoz
portavoz@bigfoot.com

****
[3x07] Hackmeeting 2002 / Madhack'02 by green
****

Hackmeeting 2002 / Madhack'02

Vuelve con fuerza la hackmeeting en su tercera convocatoria, esta vez teniendo lugar en la capital de Espanya. La gente de SET no asistio a la segunda que tuvo lugar en Leioa pero si lo hicimos a esta de Madrid.
La HM de este ano defraudo, quiza hubo incluso demasiada gente en ciertos momentos pero parte del exito fue gracias a la organizacion de la gente del Laboratorio 03 y de la gente que vino unos dias antes para organizarlo todo. Visitamos el lab03 el fin de semana anterior a la HM y esta irreconocible.

http://www.sindominio.net/madhack02/madhack.html

El lab03 es un edificio en Lavapies a unos minutos caminando de embajadores en Madrid, es una CSOA si quereis tener mas informacion sobre el tema aqui teneis su url.

http://www.sindominio.net/laboratorio

La organizacion fue exquisita, el unico problema fue la cantidad de prensa que habia, mucho politiqueo pero vamos el resto muy bien. Intercambio de informacion
y conocer gente nueva que es la clave de estos eventos. Las hackmeetings no son lan parties, dado que la red se caia cada dos por tres y no habia corriente electrica sufiente para todos los ordenadores alli presentes. En algun momento habia bastante mas de 300 personas, teniendo en cuenta que el edificio tenia tres plantas habiles para charlas y talleres.

La sala de cine fue todo un exito aun siendo incapazes de mantener los horarios de visionado. La sala principal era un continuo ir y venir de gente a todas horas. Uno de los denominadores generales era el WiFi o 802.11b dado que el lab03 tiene red wireless. Vamos a ver un poco que ocurrio durante el Madhack'02.

La HM estaba repartida en 4 salas, Cine, Espontaneos, Petras y Sala de Fiestas siendo las dos ultimas las mas grandes. Algunas de las peliculas proyectadas fueron las siguientes :

Wargames
Tron
CUBE
Matrix
PI
23
2001
Blade Runner
Johnny Mnemonic
Ghost in the shell
Antitrust

Obviamente era imposible asistir a todo, dado el hecho de que varias charlas y talleres eran a la vez. Aqui citare lo que fue mas relevante, entre varios que asistimos.

- Desarrollo de shellcodes para exploits en linux/x86 estuvo muy bien aunque no era nada nuevo, bien presentada y amena.

- Hack Labs una de las mejores, con estilo y una charla clave por Cielito Lindo.

- FreeBSD, introduccion y cosas basicas.

- Seguridad en Debian Gnu/Linux, interesante pero no nos trajo nada nuevo abordo.

- La libertad de informacion en la educacion, algo clave, teneis que escucharla esta en la web en ogg.

- Virus en asm, bien preparada, explicando todo y muy interesante.

- LSSI, que mas hace falta decir ? La LSSI y la Politica de retencion de datos. En ogg.

- Madrid Wireless la gente de MW estuvieron prensente con varias charlas, las mas interesante si lo que te gusta es el WiFi.

- Hacktivismo y que se yo fue una de las que mas me gusto, viniendo uno de los fundadores de hactivist.com desde usa para hablar. El susodicho era Nathan que al final si aparecio.

- Que es LINENOISE ? por nuestros colegas de LN. mas info en el articulo sobre la Linenoise en proximo SET.

- Are you a cyberpunk ? Apogeo y caida de Mondo 2000 ponencia disponible en ogg merece la pena bajarsela.

Hubo alguna charla mas pero esto es lo mas destacable. Hubo un ambiente excelente en la Hackmeeting de este ano y todo el mundo se quedo con ganas de mas. La organizacion hizo todo lo que estuvo en su mano, se podia comer alli, se podia beber en la barra a precios amigos. El Chill out y las distintas sesiones que hubo viernes y sabado amenizaron el tema cantidad. Luego la gente que necesito dormir alli no tuvieron problemas y hubo sitio mas que de sobra. Esperemos que no cierren el Lab03 de Lavapies dado que da una vida increible a la zona, un ejemplo a seguir. No debemos olvidar que en esta ocasion hubo merchandising para la ocasion, desde sudaderas de HM hasta camisetas pasando

por alfombrillas de raton de todo tipo. Fue un evento a seguir y repetir. Desde aqui os invito a que visiteis la Hackmeeting el proximo ano.

Habia gente clasica de siempre amigos de SET en el evento y algunos italianos muy majos, lo que demuestra que las hackmeetings si mueven a gente de fuera. Saludos a todos la gente del Laboratorio.

Green

EOF

-[0x04]--
-[Eggdrops I y II]---
-[by sicario]---SET-26-

IRC Bots - Eggdrops

Vamos a tratar sobre del robot para IRC mas popular, el Eggdrop. Este robot esta creado bajo sentencias de C, existiendo versiones tanto para Unix/Linux asi como para el windows, como es de suponer, aquí solo trataremos de la version para Unix/Linux. Nos basaremos en la version 1.6.3

1.Requerimientos :

- Una cuenta Shell, con permisos para compilar y ejecutar programas.
- Cerciorate de tener el TCL instalado en tu maquina:
  Utiliza el comando tclsh para cambiar al shell del TCL y verificar si lo
  tienes instalado.

Podras descargar la ultima version del TCL de
  ftp://ftp.scriptics.com/pub/tcl

El TCL es un lenguaje para crear scripts, desarrollado por John Ousterhout, algunas distribuciones de Linux vienen con el TCL ya instalado.

2.Descarga del Software :
  Hay muchos lugares de donde puedes descargar el archivo comprimido del
  Eggdrop. Aqui alguno de ellos :

http://www.eggdrops.net/
http://www.eggheads.org/
http://www.egghelp.org/

3.Instalacion :
Una vez descargado, procede a descomprimirlo :
  #tar -zxvf eggdrop1.6.3.tar.gz
Ahora ingresas al directorio del archivo descomprimido :
  #cd eggdrop1.6.3
y procedes a configurarlo y compilarlo.
  #./configure
  #make config
  #make

Con esto ya tienes instalado el eggdrop en tu sistema, ahora tendras que crear un robot con las necesidades que requieras. Lo ideal es tener agrupado los bots que vayas a crear por directorios, en el caso de que vayas a instalar mas de uno.

Suponiendoce que nuestro robot se ira a llamar Bot y nuestro home directory sea \home\robot

  #make install DEST="\home\robot\Bot"

Esto creara un directorio dentro de nuestro home llamado Bot, donde tendremos que editar el archivo de configuracion para nuestro robot. Encontraras uno como ejemplo llamado eggdrop.simple.conf. Editalo con tus requerimientos y renombralo para mayor facilidad de uso.

A continuacion te pongo un archivo de configuracion, con parametros creados para el servidor de IRC Dalnet :

```
#En esta linea configuras la ruta donde se encuentra el binario
#del Eggdrop.

#! /home/robot/bot/eggdrop

#Aqui configuras el Nick del robot y su password en variables
#que se utlizan luego.

set eggnick "Bot"
set botpass "password"

#Aqui configuras los datos generales del Bot.

set username "Robot"
set admin "sicario <sicario@sicario.net>"
set network "DALnet"
set timezone "EST"
set offset "5"

#Si deseas tener logs de tu canal, los configuras aqui.

set max-logs 5
set max-logsize 0
set quick-logs 0
logfile mco * "sicario.log"
logfile jkp #canal "/home/robot/bot/logs/Bot.log"
set log-time 1
set keep-all-logs 0
set switch-logfiles-at 300
set quiet-save 0
set console "mcobxs"

#Aqui configuras el nombre del file de usuarios del bot y las
#rutas de ayuda, temporales, del MOTD y del banner al hacer
#telnet o un dcc chat al robot.

set userfile "Bot.user"
set sort-users 1
set help-path "help/"
set temp-path "/tmp"
set motd "motd"
set telnet-banner "telnet-banner"

#Aqui configuras los datos de tu bot si estara linkado a
#otros bots.

set botnet-nick "Bot"
listen 4567 all
set protect-telnet 1
set dcc-sanitycheck 0
set ident-timeout 6
set require-p 0
set open-telnets 0
set stealth-telnets 0
set use-telnet-banner 1
set connect-timeout 15
set dcc-flood-thr 6
set telnet-flood 5:5
set paranoid-telnet-flood 0
set resolve-timeout 20
```

```
##### MORE ADVANCED STUFF #####

set ignore-time 10
set hourly-updates 00
set owner "sicario"
set notify-newusers "sicario"
set default-flags "hp"
set whois-fields "url birthday"
set remote-boots 0
set share-unlinks 0
set die-on-sighup 0
set die-on-sigterm 0
set must-be-owner 1
set max-dcc 50
set dcc-portrange 1024:65535
set enable-simul 1
set allow-dk-cmds 1

#Aqui configuras la ruta de los modulos. Los modulos son
#sentencias adicionales en C, que te proporcionan
#utilidades fuera del propio eggdrop.

set mod-path "modules/"

#Aqui levantas el modulo de canales y lo configuras.
loadmodule channels
set chanfile "bot.chan"
set ban-time 300
set exempt-time 60
set invite-time 60
set force-expire 1
set share-greet 0
set use-info 1

#Lo que sigue son los parametros globales para control de
#canales.

set global-flood-chan 6:6
set global-flood-deop 0
set global-flood-kick 0
set global-flood-join 0
set global-flood-ctcp 6:6
set global-chanset {
        -clearbans      -enforcebans
        +dynamicbans    +userbans
        -autoop         -bitch
        +greet          +protectops
        +statuslog      -stopnethack
        -revenge        -secret
        +autovoice      +cycle
        +dontkickops    -wasoptest
        -inactive       +protectfriends
        -shared         -seen
        +userexempts    +dynamicexempts
        +userinvites    +dynamicinvites
}

set global-chanmode "nt"

#Si deseas tener un canal especifico con protecciones distintas
#las adicionas a partir de aqui.
```

```
channel add #canal {
  chanmode "+nt"
  idle-kick 0
  need-op { needop "#canal" }
  need-invite { needinvite "#canal" }
  need-unban { needunban "#canal" }
  need-key { needinvite "#canal" }
  need-limit { needinvite "#canal" }
  flood-chan 6:6
  flood-deop 0
  flood-kick 0
  flood-join 0
  flood-ctcp 6:6
}

channel set #canal -clearbans -enforcebans +dynamicbans +userbans +userinvites
channel set #canal -autoop -bitch +greet +protectops +protectfriends
channel set #canal -stopnethack -revenge +autovoice -secret -shared +cycle
channel set #canal +dontkickops -wasoptest -inactive -seen +statuslog

#estos son algunos procesos que se ejecutan automaticamente si
#el robot necesita Op, necesita ser invitado al canal o
#quitarce un ban.

proc needop {channelname} {
global botnick nick botpass eggnick
putserv "PRIVMSG NickServ :identify $eggnick $botpass"
putserv "PRIVMSG ChanServ :op $channelname $botnick"
}

proc needinvite {channelname} {
global botnick nick botpass eggnick
putserv "PRIVMSG NickServ :identify $eggnick $botpass"
putserv "PRIVMSG ChanServ :invite $channelname $botnick"
}

proc needunban {channelname} {
global botnick nick botpass eggnick
putserv "PRIVMSG NickServ :identify $botpass"
putserv "PRIVMSG ChanServ :unban $channelname all"
}

#Aqui levantas el modulo de servidor y lo configuras.
loadmodule server
set net-type 3
set nick "Bot"
set altnick "Bot_"
set realname "http://home.dal.net/sicario/"
set init-server { start }
proc start {} {
global botnick botpass eggnick
putserv "NickServ IDENTIFY $eggnick $botpass"
putlog "Identifying to NickServ (Auto-Identification)"
putserv "MODE $botnick +iw-xs"
}

#Aqui configuras la lista de servidores al cual se conectara el
#robot.
set servers {
  tsunami.dal.net
  ced.se.eu.dal.net
  paranoia.se.eu.dal.net
```

```
}
set keep-nick 1
set use-ison 1
set strict-host 0
set quiet-reject 0
set lowercase-ctcp 0
set answer-ctcp 3
set flood-msg 3:3
set flood-ctcp 3:3
set never-give-up 1
set strict-servernames 0
set default-port 6669
set server-cycle-wait 10
set server-timeout 10
set servlimit 0
set check-stoned 0
set use-console-r 1
set debug-output 0
set serverror-quit 0
set max-queue-msg 350
set trigger-on-ignore 0
set double-mode 1
set double-server 1
set double-help 1

#Aqui levantas el modulo para CTCP eventos.
loadmodule ctcp
set ctcp-version "Eggdrop 1.6.3 admin: sicario"
set ctcp-finger "Eggdrop 1.6.3 admin: sicario"
set ctcp-userinfo "Eggdrop 1.6.3 admin: sicario"
set ctcp-mode 2

#Aqui levantas el modulo para IRC.
loadmodule irc
set bounce-bans 1
set bounce-modes 0
set kick-bogus-bans 0
set bounce-bogus-bans 1
set max-bans 45
set max-modes 45
set allow-desync 1
set kick-bogus 0
set ban-bogus 0
set kick-fun 0
set ban-fun 0
set learn-users 0
set wait-split 600
set wait-info 1
set mode-buf-length 200
set no-chanrec-info 1
set revenge-mode 1

set bounce-exempts 0
set bounce-invites 0
set max-exempts 20
set max-invites 20
set bounce-bogus-exempts 0
set kick-bogus-exempts 0
set bounce-bogus-invites 0
set kick-bogus-invites 0
set prevent-mixing 1
```

```
##### TRANSFER MODULE #####

#loadmodule transfer
#set max-dloads 2
#set dcc-block 0
#set copy-to-tmp 1
#set xfer-timeout 35

##### SHARE MODULE #####

#loadmodule share
#set allow-resync 1
#set resync-time 900
#set private-owner 1
#set private-global 1
#set private-globals "mnot"
#set private-user 1

##### FILESYSTEM MODULE #####

#loadmodule filesys
#set files-path "/home/robot/bot/filesys"
#set incoming-path "/home/robot/bot/incoming"
#set upload-to-pwd 0
#set filedb-path ""
#set max-file-users 2
#set max-filesize 700000

##### NOTES MODULE #####

loadmodule notes
set notefile "seafish.notes"
set max-notes 5
set note-life 90
set allow-fwd 1
set notify-users 1
set notify-onjoin 1

##### CONSOLE MODULE #####

loadmodule console
set console-autosave 1
set force-channel 0
set info-party 1

##### WOOBIE MODULE #####

# this serves absolutely no purpose and is for demonstrative
# purposes only
#loadmodule woobie

##### SEEN MODULE #####

##### BLOWFISH MODULE #####

checkmodule blowfish

##### ASSOC MODULE #####

# uncomment this line to load assoc support, i.e naming channels on
```

```
# the botnet
#loadmodule assoc

##### WIRE MODULE #####

# this module provides all the standard .wire commands via dcc.
# it's an encrypted partyline communication tool, compatible with wire.tcl
# uncomment this line to load it
#loadmodule wire

#Aqui colocas los scripts que vayas a usar, estos son algunos
#ejemplos. Recuerda que los scripts necesitan alguna
#configuracion adicional en el eggdrop o en el mismo script,
#lee la ayuda de cada script.

source scripts/bnc.tcl
source scripts/randversion.tcl
source scripts/bseen.tcl
source scripts/responde.tcl
source scripts/count.tcl
source scripts/ping.tcl
source scripts/chatstats.tcl

--------- End
```

Una vez que hayas terminado de editar el archivo de configuracion, procedes a ejecutar el robot, como esta sera la primera vez, tendras que usar la siguiente linea de comando :

```
  #./eggdrop -m conf
```

Suponiendoce que hayas renombrado el archivo eggdrop.simple.conf por conf

Una vez que el robot se haya conectado, procedes a enviarle un privado por el IRC, poniendo la siguiente linea :

```
  /msg Bot hello
```

El bot te reconocera como su propietario u Owner, procedes a configurar tu clave

```
  /msg Bot PASS tuclave
```

Ahora le haces un DCC Chat, pones tu clave y digitas .die , todos los comandos del robot dentro del Chat son precedidos por un . como indicador de comando. Tambien puedes matar el PID del proceso ejecutandoce del Bot.

```
  #kill -9 <#PID>
```

Luego de haber echo esto, procedes a ejecutar el robot sin necesidad de poner el parametro -m

```
  #./eggdrop conf
```

Aquí te muestro los parametros para ejecucion del bot :

```
    -n   Ejecuta el robot en modo no background, mostrandote todos los
         procesos del bot en la terminal de la consola.
    -nt  Ejecuta el robot en modo no background, mostrandote un entorno
         parecido al ircII.
    -nc  Ejecuta el robot en modo no background, mostrandote informacion
         del canal cada 10sg.
    -m   Se utiliza la primera vez en la ejecucion de un eggdrop, para
```

```
         crear el archivo de usuarios.
    -v   Solo muestra la version del eggdrop al momento de desconectarce.

Niveles de acceso al robot.
Los comandos  que puedas  ejecutar tanto  por DCC  chat como  por MSG,  estan
definidos de acuerdo al nivel de acceso que tengas al robot.

    n  (owner)  es el creador del robot, el maximo nivel.

    m  (master) tiene acceso a adicionar/eliminar/modificar
       usuarios en el canal.

    o  (op)      Puede tener estado de operador en el canal.

    d  (deop)    No puede tener estado de operador en el canal.

    k  (kick)    Un usario con este flag, es automaticamente
       expulsado del canal.

    f  (friend)  Este flag indica estar en la lista de Friends
       del robot.

    a  (auto-op) El robot da automaticamente el modo de
       Operador al entrar al canal, siempre en cuando el parametro
       autoop de la configuracion este +autoop

    v  (auto-voice) El robot da automaticamente el modo de
       Voice al entrar al canal, siempre en cuando el parametro
       autovoice de la configuracion  este en +autovoice

Para visualizar los comandos a los que tienes acceso, solo digita .help

Comentarios/sugerencias a :

sicario@phreaker.net



--------------------------------------------------------------------------
-[ Eggdrops  II]-----------------------------------------------------------
--------------------------------------------------------------------------

--------------------------------------------------------------------------
     Comandos, BotNet, File Server y Scripts en el IRC Bot Eggdrop

Continuando con nuestros temas relacionados al IRC, en el numero anterior
explicamos como configurar, instalar y poner en linea un Eggdrop para Linux.
Ahora veremos como usar ese robot, comandos basicos, BotNet y uso de Scripts.

Comandos
--------
Algunos robots usan scripts para aceptar comandos mediante simples msg o
querys, comandos para administracion y control de un canal, llevar
estadisticas y otras utilidades. Lo mas recomendable es separar esos accesos,
el eggdrop viene por defecto para utilizar comandos de administracion solo
por DCC Chat, debido a la seguridad de los passwords y usuarios, es
preferible dejar que eso trabaje asi, los demas procesos como estadisticas u
otras utilidades, estan orientados al uso de cualquier usuario, entonces lo
logico es que trabajen por medio de msg o comandos públicos, luego hablaremos
de algunos de esos scripts.

Comandos de DCC Chat
```

Los comandos usados en un dcc chat van precedidos del .
Tomaremos como nombre del robot: Black-Dragon
Al costado de la sintaxis de cada comando colocare el atributo minimo requerido para acceder a dicho comando, separado por un |. Ejemplo

```
adduser <nickname> <channel> | +m
------- --------------------   --
comando     parametros         atributo
----------------------------
          sintaxis
```

+n <= owner
+m <= master
+o <= operador
+t <= botnet master

adduser <nickname> <channel> | +m
Este comando es usando para añadir un usuario, siempre en cuando este se encuentre en el canal, monitoreado por el robot.
El robot automaticamente tomara los datos que necesita del info del usuario en linea, es decir no habra necesidad de indicarle cual es su user id ni su hostmask.

Ejemplos
        .adduser sicario

Al anyadir un usuario tendras que asignarle atributos, ya sea owner, master u operador, con el comando .chattr , si no configuras eso, el usuario no podra usar ningun comando.
Luego de asignarle un nivel, el usuario tendra que configurar su clave, enviando un mensaje con el comando pass <password>

Ejemplos
        /msg Black-Dragon pass zasd763j <= Este comando es mediante msg

Una vez hecho esto, el robot confirma la configuracion de la clave enviando un notice al nuevo usuario, para poder enviarle un Dcc Chat y entrar en el party line del robot.

away [away-message] | all users
Funciona de la misma manera que el AWAY del IRC, solo que el estado de away es marcado en el party line del robot, el mensaje de away es mostrado si algun usuario utiliza el comando .who, para marcar tu retorno puedes utilizar el comando .back o simplemente .away sin mensaje alguno.

Ejemplos
        .away No estoy.

back | all users
Desactiva tu estado de away.

Ejemplos
        .back

backup | +n
Se utiliza para realizar un backup de la lista de usuarios.

```
bans all
Muestra la lista de bans activos y los bans permanentes del robot.

Ejemplo
        .bans all

+ban <channel> <hostmask> <reason>      | +m
Este comando es similar a un auto kick ban, es decir el ban que se coloque es
permanente, y solo puede eliminarlo un usuario que tenga como atributo minimo
+m.

Ejemplos
        .+ban #CDLR *!*@200.37.2.* Spammer      <= Coloca un ban permanente a
                                                   todo el dominio 200.37.2.*
                                                   y con una razon.
        .+ban *shit*!*@* No eres bienvenido     <= Coloca un ban a todo aquel
                                                   que use como user id
                                                   *shit* o trate de usar
                                                   dicho texto como nickname.

El modo de colocar los parametros de este comando es el mismo a un /ban,
un /mode +b en el irc, puedes usar muchas variantes para el hostmask
dependiendo de que tanto quieras evitar el ingreso de alguien.


-ban <hostmask/number>          | +m
Utilizado para borrar un ban permanente o temporal, de la lista de baneados
del robot.

Ejemplos
        .-ban 1                 <= Borra el ban numero 1 de la lista.
        .-ban *shit*!*@*        <= Borra el ban que cumpla *shit*@* como
                                   hostmask.

banner <text>           | all users
Muestra un mensaje a todos los usuarios conectados al bot en el party line.

Ejemplos
        .banner El bot sera desconectado por unos momentos


boot <nickname> [reason]
boot <nick@bot> [reason]        | +t
Expulsa a un usuario de el party line, con un mensaje opcional.

Ejemplos
        .boot sicario fuera!


chattr <nickname> [attributes] [channel]        | +m
Sirve para asignarle o quitarle atributos a un usuario, globalmente si el bot
esta en varios canales, o en un canal determinado.

Ejemplos
        .chattr sicario +m          <= Anyade a sicario como master global, es
                                       decir en todos los canales
                                       monitoreados por el robot.
        .chattr sicario -o #CDLR    <= Quita el nivel de operador a sicario
                                       en el canal #CDLR.
        .chattr sicario -m|+o #CDLR <= Quita el nivel de master globalmente y
                                       da el atributo de operador en el canal
                                       #CDLR a sicario.
```

Para ver la lista de atributos puedes usar el comando .help whois

- Solo el creador del robot puede anyadir y remover usuarios con atributos
  "n" (owner), "m" (master) y "t" (botnet masters).

chnick <oldnick> <newnick> | +t
Cambia el nick de un usuario registrado en el robot.

Ejemplos
        .chnick sicario daemon

chpass <nickname> [newpassword] | +t
Cambia el password de un usuario.

Ejemplos
        .chpass sicario Xfrt45fd

die [reason] | +n
Finaliza la ejecucion del robot. Si no especifias una razon, saldra el nick
de el usuario owner que ejecuto el comando, como razon del die.

Ejemplos
        .die Fuera de linea por mantenimiento

+host <nickname> <hostmask> | +m
Anyade un hostmask al registro de un usuario en el robot. Se usa este comando
cuando un determinado usuario, modifica su user id o el sitio de donde se
conecta.

Ejemplos
        .+host sicario *!epic@*.sicario.org

Existe el comando ident, que se utiliza para autentificarse con el robot
mediante un msg.
Sintaxis del comando /msg <botname> ident <clave>
El unico requisito para usar este comando, es usar el nick con el que estas
registrado al robot o ignora el mensaje que le envies.

Ejemplos
        /msg Black-Dragon ident 87653   <= Este comando es un simple msg.

Con esto el robot anyadira automaticamente tu nuevo hostmask y podras enviarle
un Dcc Chat y entrar al Party Line.

-host <nickname> <hostmask> | +m
Remueve un hostmask de un usuario en el robot.

Ejemplos
        .-host sicario *!newbie@*.tux.org

+ignore <hostmask> [comment] | +m
Anyade un host a la lista de ignorados, con tu nickname y un comentario como
datos adicionales. Este ignore es permanente, asi que no expira

```
automaticamente, ya que es anyadido manualmente, no por alguna proteccion del
robot contra flood o generado por algun script, para eliminarlo tendras que
usar el -ignore.

Ejemplos
        .+ignore *!*@*.nobody.net      <= Ignoras a todo el que entre con ese
                                          host.
        .+ignore *!*@200.6.4.20        <= Ignoras al que entre con ese IP.
        .+ignore *Zealot*!*@* Por gay  <= Ignoras al que trate de usar como
                                          nickname Zealot o como user id
                                          Zealot. Ademas pones el motivo,
                                          asi otro usuario con nivel de Master
                                          sabra el porque del ignore.

-ignore <hostmask OR number>    | +m
Remueve un ignore de la lista de ignorados del robot. Puedes usar el numero
de ignore o la mascara con que fue anyadida.

Ejemplos
        .-ignore 3
        .-ignore *!*@200.6.4.20


ignores         | +m
Muestra la lista de ignorados del robot.

Ejemplos
         .ignores

jump <irc-server> <irc-port>
Permite hacer un cambio de servidor, si no especificas el server, saltara al
proximo de la lista, en el archivo de configuracion.

Ejemplos
        .jump
        .jump matrix.dal.net 6668

kick <channel> <nickname> <reason>      | +o
Sirve para expulsar un nick del canal monitoreado por el robot, se puede
especificar el canal, si el robot esta en varios canales, y el motivo del
Kick como parametros opcionales. Si pretendes aplicar este comando a un
usuario del robot, solo podras hacerlo con usuarios que tengan los mismos
atributos o menores que los tuyos.

Ejemplos
        .kick sicario shut up!  <= Expulsa a sicario con el mensaje
                                   "shut up!"
        .kick #CDLR sicario     <= Expulsa a sicario del canal #CDLR sin
                                   ningun mensaje.

kickban <channel> <nickname> <reason>   | +o
Se utiliza este comando para expulsar y poner un ban a un determinado nick, el
ban que se coloca es temporal, este ban expira dependiendo del tiempo que se
se especifica en el archivo de configuracion del robot. Ademas se puede
utilizar hostmasks para remplazar al nickname.

Ejemplos
        .kickban sicario shut up!       <= Coloca el ban y expulsa a sicario,
                                           con un mensaje.
        .kickban #CDLR *!*@*.org.pe     <= Coloca un ban a el dominio *.org.pe
                                           en el canal #CDLR y expulsa a todo
                                           aquel que cumpla esa condicion.
```

```
        .kickban *sicario*!*@*          <= Coloca un ban a todo aquel que use
                                           como user id *sicario* o use como
                                           nickname *sicario*


modules <botname>       | +m
Da una lista de los modulos ejecutandose en el robot.

Ejemplos
        .modules Black-Dragon

msg <channel/nickname> <message>        | all users
Envia un mensaje a un canal o nick determinado.

Ejemplos
        .msg #CDLR hola!                <= envia un mensaje al canal #CDLR
        .msg sicario Hey que tal        <= Envia un mensaje a sicario.

Este comando se utiliza para que el robot pueda enviar mensajes con su propio
nick, es decir sicario recibira un query o mensaje con el nick de Black-Dragon
no sabra que usuario del robot lo esta haciendo, siempre en cuando sicario no
sea usuario del robot.

op <channel> <nickname>         | +o
Utilizado para obtener o dar el mode de operador en un canal.

Ejemplos
        .op sicario             <= Da el modo de operador a sicario.
        .op #CDLR sicario       <= Da el modo de operador a sicario en el
                                   canal #CDLR

deop <channel> <nickname>       | +o
Quita el modo de operador. Solo se puede deopear a usuarios con igual o menos
atributos.

Ejemplos
        .deop sicario
        .deop #CDLR sicario

loadmod <module>        | +n
Pone en ejecucion un modulo.
Loads a module.

Ejemplos
   .loadmod stats


rehash          | +n

Vuelve a cargar el archivo de configuracion del robot, se usa después de
hacer cambios, editando directamente o después de cambiar valores de
variables con el comando .set al archivo de configuracion. Al hacer un
rehash el robot se actualiza, vuelve a cargar los scripts, grava los
usuarios y vuelve a cargar la lista del user file.

Ejemplos
        .rehash


say <channel> <message>         | all users
Usado para enviar mensaje con el nick del robot a un canal determinado.
```

```
Ejemplos
        .say Hola que tal
        .say #CDLR hey tengo vida! soy inteligencia artificial


unloadmod <module>      | +n
Desmonta un modulo en ejecucion.

Ejemplos
        .unloadmod stats


+user <nickname> [hostmask]     | +m
Este comando es para anyadir un usuario sin la necesidad de que este se
encuentre presente en el canal.

Ejemplos
        .+user sicario *!epic@206.138.105.10 <= Anyades a sicario como
                                                user, el cual se conecta de
                                                dicho IP y usa como user
                                                id epic.

Cuando un usuario es anyadido al robot, el registro que se crea de ese usuario
es en base a 3 datos :
1. El nick, en este caso sicario.
2. El user id, en este caso epic.
3. El hostmask.
   Si el usuario no cumple con estos tres requisitos, el robot no lo reconoce
   como user, no podra configurar su clave, ni mucho menos hacerle un chat al
   robot, para entrar al Party Line y usarlo.


-user <nickname>        | +m
Elimina el usuario especificado en el robot.

Ejemplos
        .-user sicario

voice <channel> <nickname>      | +o
Coloca el modo de +v a un determinado nick.

Ejemplos
        .voice sicario          <= Da modo de +v al nick sicario
        .voice #CDLR sicario    <= Da modo de +v al nick sicario en el canal
                                   #CDLR

El uso del +v o voice, nada mas sirve si el canal esta en modo moderado, es
decir cuando solo los operadores y los que tengan este modo +v pueden
escribir en la ventana publica del canal.

devoice <channel> <nickname>    | +o
Quita el modo +v a un nick.

Ejemplos
        .devoice sicario
        .devoice #CDLR sicario

who     | all users
Muestra una lista de los usuarios conectados en el party line con el robot.

Ejemplos
        .who
```

```
whois <nickname>        | all users
Este comando es usado para visualizar informacion de un usuario, aun si este
no esta conectado al robot en el party line. Nos da el info, comentarios,
hostmask y los atributos de dicho usuario.

Ejemplos
        .who sicario



BotNet
------

Los eggdrops tienen la habilidad de poder unirse con otros eggdrops, a esto
se le denomina BotNet, creando entre ellos una especie de pequenya red de IRC.
Esto te permite tener mas de un robot para proteger tu canal, los robots
linked pueden tener registros de usuarios comunes de forma global o de un
canal especifico.
Algunos terminos usados :
- BotNet: Termino usado para describir multiples robots conectados.
- Link  : Termino que indica el actual enlace de un robot.
- Hub   : Un eggdrops es llamado Hub, cuando uno o mas robots estan linked
          hacia él.
- Leaf  : Es un robot dentro del BotNet que no puede conectarse a mas de un
          robot.
- Share : Termino usado para describir que dos robots estan compartiendo
          usuarios.
- Share Bots : Termino para describir a varios robots compartiendo usuarios.

Flags :
        h ( hub )    : Indica que el robot anyadido es un Hub.
        a ( alternate ) : Indica que el robot es un Hub alternativo, si por
                          algun caso tu robot no puede conectarse al hub,
                          tratara de conectarse al hub con el flag alternate.
        l ( leaf )   : Indicas que tu robot solo hara un link a un robot.
        r ( reject ) : Un robot con este flag rechaza cualquier intento de
                          enlace.
        s ( shared ) : Indica que puedes compartir el registro de usuarios
                          con el bot anyadido.

Comandos del BotNet :

+bot <bot>
```

EOF

-[0x05]----------
-[Hackers VS Pedofilia]----------
-[El reberendo]----------SET-26--

NOTAS IMPORTANTES:
Despues de mas de 6 anyos ya nos vamos conociendo todos, y tambien vosotros a nosotros... No es costumbre de SET hacer eco o publicidad de cronicas sociales por mucho polvo que levanten si estas no estan directamente relaccionadas con la informatica, pero en esta ocasion hemos hecho una excepcion por la importancia del tema: PEDOFILIA.

Algunos de los miembros de SET (cada dia mas viejos) somos padres (o madres), y este es un tema que nos sensibliliza mucho, por eso cuando recibimos un correo de 'el reberendo' hemos creido que el tema realmente merecia la pena, esta es la razon por la que ahora mismo estas leyendo este articulo y aunque este articulo no es realmtente tecnico, si no mas bien una peticion de ayuda contra la pedofilia, lo hemos incluido encantados.

Por otra parte, tambien me gustaria mencionar que durante la elaboracion de este articulo (mas bien cuando se estaba acabando), 'el reberendo' sufrio un accidente de coche y no hemos sabido nada mas de el.

Ahora si, ya puedes leer este articulo.

El editor.

HACKERS VS PEDOFILIA

La pornografia infantil es la peor lacra que tiene Internet. Se calcula que uno de cada dos delitos que se cometen en la Red tienen que ver con el abuso sexual de los ninyos, y esto es mucho decir teniendo en cuenta los delitos informaticos. Pornografia infantil es la reproduccion explicita de imagenes sexuales de un ninyo o una ninya. Se trata, en si misma, de una forma de explotacion sexual de los ninyos, y desde luego no hace mucha falta convenceros de esto. Estimular, enganyar o forzar a un ninyo para posar en fotografias o para participar en videos pornograficos es ultrajante y supone un menosprecio de la dignidad y la autoestima de los ninyos.

Somos, (o mas bien estamos formando) un pequenyo team que en estos momentos esta estructurandose y que solamente y de momento consta de 4 miembros, el "DHM Team".

Nuestro principal deseo y preocupacion es acabar con todo tipo de contenido de caracter pedofilico, y es por ello por lo que en la medida de lo posible pedimos ayuda a SET y sus lectores, es decir, si pretendeis entrar en un Team, perteneceis a uno o actuais solos... no importa, lo importante es luchar contra un enemigo en comun.

Si crees que tus conocimientos "no llegan" para poder luchar contra la pedofilia te equivocas, desde nuestra web trataremos de ensenyar en la medida de lo posible a otros hackers sin importar en lo que puedan ayudar, lo importante es arrimar el hombro en este tema, hay muchas labores por desarrollar. Esta es una de las causas mas nobles de utilizar vuestros conocimientos y por la cual en muchos casos los adquiristeis, no lo penseis mas y arrimar el hombro, prestarnos vuestra ayuda en este tema, esta no es una colaboracion igual a la que podeis hacer en otros sitios, NO!, esto es mucho mas importante, y solamente es una union para proteger a tu hermano, hijo o familiar y desde luego no es excluyente de vuestras actividades o proyectos propios y cotidianos.

Por esta razon somos un grupo absolutamente transparente respecto a cualquier tipo de ayuda solamente necesitamos colaboracion para poder luchar en contra de esta lacra social que circula por la red, En ningun momento buscamos protagonismo, rivalidad u otras razones ajenas a nuestra voluntad, y por esto, todo el q lo desee y pueda ayudarnos y/o colaborar con nosotros sera recibido con la gratitud y entusiasmo que corresponde a tan magnifica ayuda, solamente nos interesa la colaboracion desinteresada por un tema que si es de interes.

Por este motivo nosotros no nos podemos ni queremos quedar impasibles ante esta barbarie e intentamos reaccionar y actuar siguiendo unas determinadas pautas.

Para que os hagais una idea de las labores que intentamos llevar a cabo (siempre en medida de lo posible) aqui os las expongo para que podais ver en que consiste nuestro trabajo.

NUESTRA MISION Y OBJETIVOS

- Mirar, rastrear, buscar, indagar, investigar todos los sitios web que los spiders identifiquen como material adulto, proveniente desde america del sur, preferentemente servidores chilenos.

  Para los mas neofitos, un Spider es un programa rastreador, que busca segun unos patrones. En este caso introducimos patrones como si los pedofilos "fueramos nosotros", como si nosotros fueramos los que estamos buscando este tipo de pornografia.

  Actualmente nuestra busqueda esta restingida, por decirlo de una manera al protocolo TCP/IP

- Rastrear movimientos ejecutados en esos servidores "marcados" ya sea a nivel usuario como de administracion.

- Tratamos de infiltrarnos en todo tipo de archivos bajo denominacion de imagen o video. gif, jpg, mov, mpg, avi, mpeg, o cualquier otro tipo de fichero se surja.

- Rastrear todo tipo de protocolo de transferencia P2P FTP con nombres de archivos bajo denominaciones de imagen o video que parezcan sospechosos.

  Actualmente, las redes P2P nos estan causando nuevos problemas dado que ahora tambien tenemos que busar en estos lares, necesitamos ancho de banda! la tuya.

- Rastreamos tambien (o eso tratamos) a usuarios que "consumen" este tipo de pornografia

- Analizamos los archivos obtenidos y su exacta procedencia, host, usuarios, fechas, movimientos...

- Mantener una lista de usuarios y administradores sospechosos de tenencia, o administracion de archivos pedofilicos ya sea para uso personal como para posteriores manipulaciones e incluso publicaciones via internet.

- Por supuesto no nos limitamos a descubrir a los usuarios y administradores de archivos pedofilicos, tambien comprobamos y confirmamos el delito y archivamos los correspondientes medios de pruebas del acto delictivo.

- Tratamos de localizar al delincuente pedofilico y su exacta ubicacion fisica por medio de rastreos tecnicos propios (que tratamos de no comentar para que los delincuentes no tomen medidas, no por otra razon)

de nuestra organizacion bajo tecnologia propia, para tratar de obtener asi un 100% de exactitud para su eventual arresto el cual estara a cargo de las AUTORIDADES PERTINENTES

ACCIONES

Lo que normalmente hacemos una vez enconrados los delincuentes, es tratar de comprobar la existencia real de contenido pedofilo, elaborar un pequenyo dosier con la informacion mas relevante como alojamiento, host, y todo lo que tengamos en nuestras manos para con ello poder denunciar esto con el mayor numero de detalles y facilitar el transito de las correspondientes acciones legales.

COMO DENUNCIAMOS

Una vez realizadas la tareas antes mencionadas nos ponemos en contacto con las autoridades pertinentes mediante sus sites web o via telefonica con los responsables de los departamentos especificos, para comunicarles de la existencia de estos sites y de la informacion recabada al igual que exigimos una pronta accion o en su defecto los motivos por los que no puede darse esta (en algunos casos, las autoridades prefieren esperar a intervenir porque asi pueden cazar a mas gente, o a una red entera).

A continuacion os cito alguno de los lugares donde nosotros denunciamos estas cosas y donde vosotros y vosotras podreis tambien denunciar con facilidad.

ACPI (Asociacion Contra la Pornografia Infantil)
http://www.asociacion-acpi.org
<a.acpi@terra.es>
Apdo. de correos 43. Villaviciosa de Odon. 28670-Madrid
Telefono: 916 166 917
Fax: 918 594 455

Defensa al Menor (Organización en defensa del menor con sede en Madrid
desde 1997)
http://www.dmenor-mad.es
<defensor@dmenor-mad.es>
Telefono: 915 634 411.

Internet Child Center (Organización Americana sobre regulación de
Pornografia infantil en la Red)
http://www.icc-911.com

FSM (Asociación alemana que supervisa denuncias sobre webs
ilegales en Alemania)
http://www.fsm.de

Si te gusta trabajar por libre, estas dos direcciones pueden ser un buen punto de comienzo:

Direccion general de la policia. Aqui podras encontrar la legislacion en Espanya sobre la pedofilia en Internet.
http://www.mir.es/policia/uiti/legisla.htm

El amor es mas fuerte, un buen punto de comienzo para adentrarse en las redes anti-pedofilia.
http://www.elamoresmasfuerte.com

LOS RESQUICIOS LEGALES DONDE SE PARAPETAN LOS PEDOFILOS.

Es realmente dificil lograr una aplicacion efectiva de las leyes contra una actividad encubierta. Pero las leyes deben ser aplicadas. Son la proteccion final de los ninyos y hasta ahora no se ha hecho lo suficiente para promulgar leyes realmente eficaces o para aplicarlas cuando ya esten en vigor.

Pero las leyes varian en cada pais y esto es sabido por estos delincuentes que utlilizan esto para quedar impunes de sus horribles actos, asi pues, el mayor resquicio sobre este tema es el establecido en algunos paises, donde a este tipo de delito no se le considera como tal, ya que se ampara en el derecho a la utilizacion de imagenes o fotos con caracter artistico (Humillante desde nuestro punto de vista) independiente de su contenido.

COMO ACTUAR EN ESTE CASO

En el momento en que la acciones legales pertinentes llevadas a cabo contra este contenido no pueden obtener resultados positivos, nosotros optamos por la segunda via que consiste en grupos de apoyo hacker-antipedifilia. Si las leyes no protejen a los ninyos, los hackers lo haremos, si somos capaces te tirar servidores tremendamente protegidos, estos tambien caeran, podran levantarlos otra vez, pero volveremos a tirarlos.

Somos conscientes que esto no es de ningun modo legal, pero si nadie proteje a nuestros hijos nosotros lo haremos.

Esto para nosotros es un gran paso ya que nos permite de una manera totalmente anonima el uso de una ayuda inestimable que nos es brindada de forma desinteresada por TEAMS hackers o independientes, sensibilizados por este tema y que demuestran que lejos de los encasillamientos sociales los conocimientos adquiridos son utilizados para acciones en post de la dignidad humana y que su condicion dista mucho de la idea preestablecida y se acerca mucho mas a la de "heroes anonimos" dispuestos a proteger y servir a los derechos de los mas debiles (Los ninyos y ninyas).

NUESTRO PREMIO

Desde luego, nosotros no queremos ni buscamos ningun tipo de remuneracion ni reconocimiemto publico, pero realmente lo obtenemos: Os aseguro que trabajando en esto sentimos que hacemos algo bueno por los demas.

En todo caso,nosotros revindicamos que jamas se hable mal de la comunidad hackers porque ensucian nuestros logros y objetivos y nosotros comprendemos que quien lo hace, lo hace solo por la ignorancia de lo que realmente es la informatica pero para que ahora lo sepan y les queden bien en claro las distintas culturas ciberneticas que existen les rogamos a esos que se informen antes de nada. (si tienen dificultades en este sentido yo personalmente estare encantado de mostrarselas).

En este punto es donde nosotros utlizamos este espacio concedido por los chicos de ’SET e-zine’ (que demuestran su gran interes y disponibilidad para luchar contra esta infame lacra), para dirigirnos a todos los lectores de este, vuestro magazine para solicitaros y pediros vuestro apoyo y lo que es mucho mas importante, vuestra inestimable ayuda para poder combatir esta repugnante miseria que nos asola y humilla con la indefension de nuestros Hermanos e hijos

Los que esteis dispuestos a arrimar el hombro, sea cual sea el tipo de ayuda, podeis encontrarnos aqui en las siguientes direccones:

Server: irc.red-latina.org
Canal: #dhmteam

```
 http://www.dhmteam.tk
 <elreberendo@hotmail.com>

 El reberendo.
```

EOF

-[0x06]----------
-[Microcodigo]----------
-[by nomellames]----------SET-26-

La actualizacion del Microcodigo en chips Intel

0. Disclaimer

Esto solo es educativo. Las actualizaciones del microcodico estan bajo el copyright de Intel, y no deben ser usadas bajo ningun otro proposito que para que el que fueron creadas, es decidir, modificaciones legitimas del microcodigo. Yo no he modificado el microcodigo, y en ningun caso he infringido el copyright.

1. Introduccion

A pesar de que mi especialidad es wardriving, mi primer articulo es sobre la actualizacion del microcodigo en maquinas Intel (Intel microcode updates). Y asi mis queridas amigas (espero que me lean solo chicas, y solteras. Mi direccion esta mas abajo) os preguntareis que tiene que ver esto con la seguridad informatica, y como vas a conseguir hackear con esto la cuenta de hotmail de tu novia(o).

Pues el caso es que el susodicho microcodigo esta encriptado, con lo cual solo Intel puede actualizar el microcodigo. En el caso de que alguien consiguiera desencriptar el microcodigo, podriamos meter nuestro propio microcodigo en el chip. Supongo....

Para que ? Con que objetivo ? Pues como en muchas ocasiones por pura diversion, ...con que derecho Intel nos esconde algo ?. Tambien tenemos otros motivos, Si Intel quiere esconder algo, ... sera por algo ? Tal vez la respuesta es simplemente que los chicos de Intel se aburren y hacen estas cosas por puro deporte y ganas de hacer trabajar las neuronas, pero dudamos de que esto sea cierto, por tanto tiene que existir una razon,....razonable. Como podreis comprobar, este es el tipico articulo-provocador que con tanto frecuencia y escaso exito se empenyan en publicar los alegres chicos de SET y sus secuaces. Queremos comprobar si hay alguien interesado y con tiempo libre para estudiar el problema.

Pero a ver, demos un poco de informacion,...

1.1 que es eso del microcodigo?

El microcodigo que inyectas en el chip sirve para actualizar las microinstrucciones. Me explico:

En el mundo de la arquitectura de ordenadores hay dos corrientes, una arquitectura RISC, y otra la arquitectura CISC.

La arquitectura RISC consta de instrucciones simples, mientras que en CISC las intrucciones son mas complejas. En CISC dirias al ordenador : "Hackea la cuenta de mi abuela y mi tia". En RISC dirias al ordenador: "Hackea. La cuenta. mi abuela. Hackea. La cuenta. Mi tia"

RISC es usado por arquitecturas como ARM y Sparc. CISC es usado por x86 (o sea, el PC de tu casa). Cual es mejor...bueno, eso es otra historia.

El caso es que de alguna manera, en los x86, esas "Instrucciones largas" han de ser mapeadas a instrucciones mas pequenyas que el ordenador pueda entender. Las actualizaciones del microcodigo cambia ese mapeo, o las microinstrucciones finales, no estoy seguro. Con ello, Intel se ahorra dinero cuando hay un bug, llamado en nomenclatura Intel "Errata". Y son muchos Bugs. Sino, haced un search sobre "processor Specification Update" en la pagina de Intel.

Un caso clasico fue el bug de la coma flotante en el primer Pentium, que puede ser resuelto con los microcodigos (Usare microcodigo solo a partir de ahora en vez de actualizacion del m...porque me canso).

El microcodigo esta explicado en el capitulo 8, seccion 10 de IA-32 Intel Architecture Software developers manual Volume 3: Systems programming guide. Lo podeis bajar de la pagina de Intel. Esta compuesto por 2048 bytes of data, 48 bytes componen la cabecera, y los restantes 2000 son el verdadero microcodigo. Los microcodigos estan encriptados, o al menos "firmados" digitalmente. Si intentas meter un microcodigo a tu ordenador que ha sido retocado, el procesador lo rechazara. Aun mas, si el microcodigo no pertence a el chip especificado al cual esta destinado, el chip tambien rechazara el microcodigo.

2. Como puedo meter un nuevo microcodigo en mi ordenador?

Normalmente la BIOS se encarga de eso. Tambien hay una utilidad por ahi que

```
permite instalar el microcodigo desde windows usando unos ficheros que INTEL
pone a disposicion de los usuarios gratuitamente,....cosa logica ya que asi
nosotros nos encargamos de hacer el trabajo que ellos debieran haber hecho.
Os imaginais una revision de todos los chips defectuosos tipo automovil ?
No, no sonyeis, esto en el mundo de los procesadores nunca va a pasar.
No se. A mi Windows no me gusta. lo siento. O sea que se poco del tema.
Afortunadamente, Linux me gusta, y en Linux si puedes actualizar el microcodigo
de forma facil y sencilla. Como? Si tienes un Kernel 2.4.X, al instalar el
kernel puedes seleccionar la opcion de usar microcodigos. Creo que en RedHat
esta seleccionado por defecto. En tu distribucion de linux, haz
        make menuconfig
y seleccionatodos todos los /dev/cpu que veas.
Luego tienes que coger el fichero ASCII con todos los microcodigos
eso lo puedes recoger de:
http://www.urbanmyth.org/microcode/
Los ficheros contienen todos los microcodigos, ademas de un controlador para el
driver. Leeros el help del controlador para ver como funciona
3- Pero como funciona el driver?
Es bastante simple. Os pongo el pseudocodigo, y luego explico las intrucciones
Mira la cabecera
        Si no es el codigo para este chip o el checksum es incorrecto
                Salta al siguiente microcodigo del fichero
        Si es entonces
        Imicializa los registros para llamar a WRMSR
                EAX contiene la direccion del microcodigo
                EDX contiene cero
                ECX contiene 79h
        Llamar WMSR (hemos actualizado el microcodigo)
Inicializa los registros para llamar a WRMSR
                EAX contiene 0
                EDX contiene cero
                ECX contiene 8bh
        Llamar WMSR (Hemos borrado lo que habia en el MSR 8bh)
        Inicializar los registros para llamar a CPUID
                EAX contiene 1
        CPUID
        Inicialiar los registros para llamar RDMSR
                ECX contiene 8bh
        Llamar RDMSR

A ver:
Los registros MSR (Model Specific registers) son usados internamente por el
procesador para diversas funciones.  Estos registros estaban bastante
undocumentados, hasta que fueron sacados a la luz de una forma un tanto
rocambolesca que no voy a explicar aqui, pero que podeis buscar en la web
(google: MSR and appendix H). O sea que al final Intel se vio forzado a
documentarlos. Yo de vosotros echaria una vistazo al tema.
Los MSR pueden ser leidos y escritos usando RDMSR y WRMSR. Una lista completa
de los MSR puede ser encontrada en
http://chip.ms.mff.cuni.cz/~pcguts/cpu/msr.txt
O sea que lo que hacemos es escribir en el MSR 79h, que es donde hacemos la
modificacion del microcodigo.
Luego reseteamos otro registro, el 8bh y llamamos a CPUID. CPUID es una
instruccion que nos ayuda a conocer nuestro amigo el procesador. Nos devuelve
diversas cosas, entre ellas que familia.tipo/stepping de procesador tienes.
Facilmente lo podreis encontrar en
http://microcodes.sourceforge.net/CPUID.htm
Pero ademas, si le pasamos las intrucciones adecuadas, CPUID nos escupira el
microcodigo que lleva dentro en 8bh.
Si el codigo en 8bh es el mismo que has metido en 79h, felicidades! tienes un
nuevo microcodigo. En /var/log/messages o usando la instruccion
dmesg|tail 10
```

aparecera el nuevo microcodigo, si es correcto, como explico mas abajo.
4- Mi aportacion
Bueno, pues para ver si el microcodigo estaba realmente encriptado, he modificado el driver para que no mire la cabecera, es decir, lo de
  Si no es el codigo para este chip o el checksum es incorrecto
        Salta al siguiente microcodigo del fichero
Me lo como. EL bicho metera lo que sea.
Desafortunadamente, a nivel de chip el microcodigo es rechazado si:
1-No es el indicado para la familia/stepping
2-Ha sido modificado
O sea, que definitivamente hay un mecanismo de seguridad dentro del chip. La gente rumorea que este mecanismo debe ser sencillo, o sino necesitariamos un numero elevado de puertas que seria prohibitivo.
He analizado un pelin los microcodigos y los que van destinados a
-Celeron los 2000 bytes son diferentes para todo los microcodigos.
-Pentium Pro los 1136 bytes son basura, puedes modificarlos y el microcodigo entrara igual, la parte final es igual para todos los microcodigos
-Pentium II y III los ultioms 1056 bytes son basura. Puedes modificarlos y el microcodigo entrara igual, la parte final es igual para todos los microcodigos
Los nuevos drivers e instrucciones de como meterlos lo podeis encontrar en:
http://microcodes.sourceforge.net
Ademas he modificado en controlador, o sea que podeis enviar el microcodigo que deseis, no el que intel os manda.
Si quereis envia pura mierda, para probar, usando mi controlador ejecutad:
dd if=/dev/urandom of=/dev/cpu/microcode bs=2048 count=1
Si teneis el driver de Tigran Aviazan, aparecera un
"No microcode found!"
Sino aparecera algo asi como "microcode updates" pero el microcodigo sera el mismo que el anterior, es decir, que el driver lo ha pasado pero el chip no ha tragado.
5- TODO
Analisis criptografico de los microcodigos, ataque de fuerza bruta (tratar de meter un numero elevado de microcodigos "forjados"
Dormir
Bueno, esto ha sido un rollo importante. Cualquier duda, queja o interes a nomellames@hotmail.com
Encriptado con mi llave si la informacion es importante. Por favor, no me encripteis chorradas. Mejor, no me envias mails con chorradas.
A proposito, mi proximo articulo sera sobre wardribing y sera mas divertido....
La clave PGP esta en el apartado 0x0E llaves PGP.
EOF

-[0x07]----------
-[Proyectos, Peticiones, Avisos]----------
-[by SET Ezine]----------SET-26--

Si, sabemos es que esta seccion es muyyy repetitiva, y que siempre decimos
lo mismo, pero hay cosas que siempre teneis que tener en cuenta, por eso
esta seccion de proyectos, peticiones, avisos y demas galimatias.

Como siempre os comentaremos varias cosas:
- Como colaborar en este ezine
- Nuestros articulos mas buscados
- Como escribir
- Nuestros mirrors
- Nuestras estadisticas
- Equipos Distribuidos
- Nuestro mailing list
- En nuestro proximo numero
- Otros avisos

-[Como colaborar en este ezine]----------

Si aun no te hemos convencido de que escribas en SET esperamos que lo hagas
solo para que no te sigamos dando la paliza, ya sabes que puedes colaborar
en multitud de tareas como por ejemplo haciendo mirrors de SET, graficos,
enviando donativos (metalico/embutido) tambien ahora aceptamos sujetadores
pero en ningun caso inferiores a la talla 80 ni de primera mano, sorprendenos!

-[Nuestros articulos mas buscados]----------

Articulos, articulos, conocimientos, conocer!, comparte tus conocimientos
con nosotros y nuestros lectores, buscamos articulos tecnicos, de opinion,
serios, de humor... en realidad lo queremos todo y especialmente si es
brillante, pero no te quedes pensando voy a hacerlo... hazlo!.
Tampoco queremos que de auto juzges, deja que seamos nosotros los que
digamos si es interesante o no.

Deja de perder el tiempo mirando el monitor como un memo y ponte a
escribir YA!.

Como de costumbre las colaboraciones las enviais aqui:
<set-fw@bigfoot.com>
<web@set-ezine.org>

Para que te hagas una idea, esto es lo que buscamos para nuestros proximos
numeros... y ten claro que estamos abiertos a ideas nuevas....

- Cisco PIX
- LSSI, articulos legales con fundamento
- Novell 6.0
- Programacion, cualquier lenguaje interesante, guias de inicio!
- Montajes y chapuzas electronicas
- Evaluacion de software de seguridad
- Hacking, craking, virus, preaking
- Evasion profesional, como escaquearse, listados de excusas
- Cronica social de tu comunidad
- Lo que tu quieras...

Tardaremos en publicarlo, puede que no te respondamos a la primera,
ni a la segunda, ni a la...(a la tercera puede que si) pero deberias

confiar viendo nuestra historia que SET saldra y que tu articulo vera la luz en unos pocos meses, salvo excepciones que las ha habido.

-[Como escribir]----------

Esperemos que no tengamos como explicar como se escribe, pero para que os podais guiar de unas pautas y normas de estilo (que por cierto, nadie cumple), os exponemos aqui algunas cosillas a tener en cuenta.

SOBRE ESTILO EN EL TEXTO:

- No insulteis y tratar de no ofender a nadie, ya sabeis que a la minima salta la liebre, y SET paga los platos rotos

- Cuando vertais una opinion personal, sujeta a vuestra percepcion de las cosas, tratar de decirlo, puede que no todo el mundo opine como vosotros.

- No tenemos ni queremos normas a la hora de escribir, si te gusta mezclar tu articulo con bromas hazlo, si prefieres ser serio en vez de jocoso... adelante, Pero ten claro que SET tiene algunos gustos muy definidos: ¡Nos gusta el humor!, Mezcla tus articulos con bromas o comementarios, porque la verdad, para hacer una documentacion seria ya hay mucha gente en Internet.

- Otra de las cosas que en SET nos gusta, es llamar las cosas por su nombre, por ejemplo, Microsoft se llama Microsoft, no mierdasoft, Microchof o cosas similares, deformar el nombre de las empresas quita mucho valor a los articulos, puesto que parecen hechos con prejuicios.

SOBRE NORMAS DE ESTILO

- Tratad de respetar nuestras normas de estilo!. Son simples y nos facilitan mucho las tareas. Si los articulos los escribis pensando en estas reglas, sera mas facil tener lista antes SET y vuestro articulo tambien alcanzara antes al publico.

- 80 COLUMNAS (ni mas ni menos, bueno menos si.)

- Usa los 127 caracteres ASCII, esto ayuda a que se vea como dios manda en todas las maquinas sean del tipo que sean. El hecho de escribirlo con el Edit de DOS no hace tu texto 100% compatible pero casi. Mucho cuidado con los disenyos en ascii que luego no se ven bien. Sobre las enyes (¤).

- Y como es natural, las faltas de ortografia bajan nota, medio punto por falta y las gordas uno entero.

  Ya tenemos bastante con corregir nuestras propias faltas.

-[Nuestros mirrors]----------

Lamentamos comunicaros que se han caido 3 de nuestros 5 mirrors, la lista de los caidos es:

http://www.vanhackez.com/SET

http://packetstorm.securify.com/mag/set

http://ezkracho.com.ar/SET

Los dos que nos quedan en pie son estos:

http://salteadores.tsx.org - USA

http://www.zine-store.com.ar - Argentina

-[Nuestras estadisticas]----------

Como mera curiosidad, y para divertimento propio, nos hemos sacado unas pequenyas estadisticas para ver como esta el tema:

Numeros: 27 (si, 27. Sacamos un numero especial)

Total bytes: 7.398.329 (Solo texto, sin contar imagenes, ni este numero!)

Articulos: 287 (Incluido este numero)

Articulistas: 97 (Sin incluir este numero)

-[Equipos Distribuidos]----------

Os acordais de la epoca en que participabamos en la colaboracion del proyecto rc5-64 en www.distributed.net?

Parece que lo han conseguido,.... con un poco de desorden y desconcierto pero lo han conseguido. El 14 de Julio de 2002 (los franceses estaran contentos) una maquina en Tokio consiguio descubrir la clave. Por si alguien le interesa la clave era,

0x63DE7DC154F4D039

y la frasecita:

"some things are better left unread"

Hasta aqui todo bien (excepto que no he sido yo quien ha ganado el premio), lo grotesco de la historia es que no se enteraron hasta el 12 de Agosto de 2002. Si estais interesados en conocer algo mas de la historia, os podeis pasar por

www1.distributed.net/pressroom/news-20020926.html

Tread ended!

-[Nuestro mailing list]----------

Imagnino que muchos ya lo habeis notado, nuestra lista de correo se ha ido al garete, de todas maneras no pasa nada porque no teniamos nada interesante que decir, lo que si os podemos anunciar es que proximamente activaremos una nueva, con la diferencia de que esta vez trataremos de hacer las cosas bien.

Mientras tanto, si vuestra incontinencia verbal a traves de Internet no os permite esperar, en nuestra web teneis un foro donde podeis desarollar vuestra incontinencia. Dicho foro se ubica en nuestra web, of course!.

http://www.set-ezine.org/

Los que querais apuntaros en la lista de correos, estaros atentos al panel
de noticias de nuestra web.

-[En nuestro proximo numero]----------

Antes de que colapseis el buzon de correo preguntando cuando saldra SET 27
os respondo: Depende de ti y de tus colaboraciones.

En absoluto conocemos la fecha de salida del proximo numero, pero en un
esfuerzo por fijarnos una fecha objetivo pondremos..... Abril de 2003

-[Otros avisos]----------

Este es un pequenyo aviso para las pocas personas que nos envian material
'fisico': CD's, revistas y cosas de esas.... (por cierto, todavia no hemos
recibido ningun paquete envuelto en billetes de euros.... a que esperais?)

El caso es que ya no disponemos de nuestro tradicional apartado de correos
o sea que todo aquel que nos quiera enviar algo 'fisico' que se ponga en
contacto previamente con nosotros por e-mail, Osea que si ardeis en deseos
de enviarnos el video de vuestro ultimo revolcon con vuestra novia, avisanos
antes.

(no me cansare de repetir las cuentas de correo)

<web@set-ezine.org>
<set-fw@bigfoot.com>

EOF

-[0x08]----------
-[Bugs para todos los gustos]----------
-[by madfran]----------SET-26--

CINCO MESES DE BUGS

INTRODUCCION

Realmente no se la causa ni motivo, pero lo cierto es que desde hace casi un anyo, me dedico a coleccionar las noticias y anuncios de seguridad que van apareciendo en la red (hay manias peores). Al archivar el ultimo bloque de papelotes y reprimiendo el impulso de hacer una gigantesca bola de papel con ellos, me he preguntado. Por que no escribir un mini articulo acerca de todo este maremagnum? Pues ni corto ni perezoso aqui me teneis explotando el tema de los exploits.

UN POCO DE ESTADISTICA

Desde Mayo de este anyo (2002 del calendario Gregoriano), me he divertido (bueno seamos sinceros, mas bien me he aburrido mortalmente) en tomar nota de todas las noticias de seguridad que caian en mis pecadoras manos por medio de los canales oficiales de distribucion de noticias de seguridad. Cuando me refiero a los canales oficiales, estoy hablando de los medios de comunicacion normales y no de los boca a boca underground que tanto abundan en la red.

La consecuencia de mi particular forma de trabajar, es que no todos las vulnerabilidades y noticias de seguridad estan aqui reflejadas, pero van a servir de base de datos de apoyo para los razonamientos y elucubraciones que bullen en mi cabeza.

A continuacion pedazo tochisimo de listado con un resumen de toda la informacion recopilada.

Microsoft SQL server
: Ataque por gusano al puerto 1433
La cuenta de admin (sa) sin pasword instalado por defecto permite ejecutar ordenes arbitrarias se SQL

Internet Explorer de Microsoft
: 12 vulnerabilidades despues de un parche que corregia 6 anteriores. Entre algunas de ellas la mas inocente permite leer archivos arbitrarios en el disco del usuario

IBM DB2
: Desbordamiento de buffer. Permite obtencion de root. El desbordamiento se encuentra en db2ckpw, que forma parte del mecanismo de autentificacion.

Excel XP Microsoft
: Permite ejecucion de codigo arbitrario. Se debe a la incorporacion de nuevas tecnologias como XML y XSLT, que realmente sirven para poco.

Ipswitch Imail 7.1
: Servidor de correo bajo Windows 2000 y XP, con desbordamiento de bufer. Permite obtencion de root. Aqui la historia viene de un problema en el servicio LDAP que permite acceso remoto.

Apache 1.3.24

Procesamiento de peticiones erroneas codificadas de forma troceada (chunked encoding). Denegacion del servicio si trabaja bajo linux y ejecucion de codigo arbitrario si se encuentra bajo Windows 2000 o NT

RAS phonebook de Microsoft

Desbordamiento de buffer. Codigo arbitrario con privilegios de administrador. Afecta a Windows 2000, XP y NT 4.0.

SQL server 2000 Microsoft

Desbordamiento de buffer. Codigo arbitrario con privilegios de administrador. El componente afectado es el SQLXML que permite a Server 2000 procesar consultas basadas en XML.

Kazaa

Problemas de configuracion por defecto. Posible lectura de cualquier archivo del disco. Problema debido a la falta de claridad de la informacion suministrada durante el proceso de instalacion.

Oracle Net Listener

Desbordamiento de buffer. Ejecucion de codigo con derechos del usuario actual debido a la erronea gestion de las peticiones encapsuladas en paquetes TNS.

Oracle 9i Application server

Desbordamiento de buffer. Ejecucion de codigo con derechos restringidos en Unix y de administrador en windows. El metodo setauth, no controla correctamente el parametro rwcgi60.

Internet Explorer de Microsoft

Ejecucion de codigo arbitrario a partir de la habilitacion de listas de carpeta en sitios ftp. El problema reside en el archivo FTP.HTT.

Internet Explorer de Microsoft

Desbordamiento de buffer en cliente gopher. Cualquier codigo con derechos de administrador. El componente de Explorer que gestiona el cliente gopher contiene el desbordamiento de buffer, cuya explotacion ni siquiere requiere la instalacion de un servidor gopher.

eDonkey 2000 v35.16.59

Programa para compartir ficheros. Desbordamiento de buffer con ejecucion arbitraria. El protocolo ed2k llama a un componente gdonkey cuyo parametro es la url solicitada. No hay ningun control sobre su contenido.

ASP.NET de Microsoft

Desbordamiento de buffer en tratamiento de cookies. El modo StateServer es el causante esta vez.

ISC BIND 9

Servidor DNSde Internet Software Consortium. Denegacion de servicio. El ataque provoca la caida del servicio named. La rutina afectada es la dns_message_findtype().

Router 3COM OfficeConnet Remote 812 ADSL

Acceso a puertos tras el router. Los puertos accesibles son tanto UDP como TCP. Los firmaware afectados son los V1.1.9 y V1.1.7.

Exchange 2000 de Microsoft
Denegacion de servicios. Debido a la mala implementacion de los RFCs 821 y 82.

OpenSSH
Protocolos SSh. Ejecucion remota. No se publicaron detalles del bug.

Excel y Word de Microsoft
Ejecucion de script HTML en hojas de estilo XSL en zona de seguridad local.

SQL server 2000 de Microsoft
Desbordamiento de buffer. La funcion OpenDataSource combinada con el MS Jet Engine es la causa del problema.

Apache 1.3.26 y 2.0.39
Ataque a traves de cabeceras incorrectas. Ejecucion de codigo bajo privilegios de administrador bajo Windows.

Macromedia Flash
Vulnerabilidad Cros Site Scripting.

OpenSSH 2.9.9 y 3.3
Desbordamiento de variable. Ejecucion de codigo con privilegios de sistema si se este usando SKEY o BSD_AUTH.

Commerce Server 2000 y 2002 Microsoft
Desbordamiento de buffer. Vulnerabilidad en filtro ISAPI Problema asociado al paquete de instalacion.

Windows Media Player
Divulgacion de informacion. Elevacion de privilegios. Ejecucion de codigo arbitrario. Se interpretan mal los scripts.

Netware DHCP Server
Denegacion de servicios. Se produce bajo Netware 6.0 SP 1

SQL Server 2000 Windows
Desbordamiento de buffer. Elevacion de privilegios por asignacion incorrecta de permisos en la llave de registro que almacena la informacion de las cuentas del servidor SQL.

CDE ToolTalk (entorno CDE UNIX)
Ejecucion de codigo arbitrario. Elevacion de privilegios.

Norton Personal Internet Firewall (Symantec)
Desbordamiento de buffer. Ejecucion de codigo arbitrario.

SQL Server 7.0 Microsoft (Procedimiento de instalacion)
Deja las contrasenyas en un archivo de texto. El origen del desafuero se encuentra en el archivo setup.iss que no es correctamente borrado despues de la instalacion.

```
Servidor JRun 4.0 de Macromedia
                        Relevacion de codigo fuente. Solo en entornos Windows
                        2000 server con IIS No se procesan correctamente
                        caracteres como %3f.jps o ?.jsp.

EA Serve (Sybase), version 4.0
OC4J (ORACLE)
Orion version 1.5.3
JRun (Macromedia) versiones 3.0, 3.1 y 4.0
HPAS (Hewlett Packard) version 3.0
Pramati version 3.0
Jo!
                        Vulnerabilidad en versiones para windows de servidores
                        de servlets J2EE. Acceso a informacion situada en
                        directorio WEF-INF.

Netware FTP SERVER
                        Denegacion de servicio. Ocurre bajo Netware 6.0 SP1 con
                        actualizacion a NWFTPD.

Internet Informacion Server 4.0 y 5.0
                        Ejecucion de codigo via .HTR.

Cisco Secure ACS Unix
                        Acceso de informacion de archivos y sistema. El
                        programa Acme.server es el causante del problema.

PHP versiones 4.2.0 y 4.2.1
                        Denegacion de servicios y ejecucion de codigo
                        arbitrario. En este caso es la peticion POST quien
                        puede emplearse para degradar el sistema.

SQL Server 2000 SP2
                        Desordamiento de buffer. Inyeccion de informacion en
                        procedimientos existentes. Error en la adjudicacion de
                        permisos de ciertos procedimientos.

Microsoft Exchange 5.5
                        Desbordamiento de buffer en codigo IMC. Generacion
                        erronea del comando EHLO.

Windows Media Player versiones 6.4, 7.1 y XP
                        Solucion a un parche anterior incompleto.

Sun RPC
                        Desbordamiento de buffer en la primitiva de filtro
                        xdr_array. Ejecucion de codigo arbitrario con
                        privilegios de superusuario.

IPSwitch Imail 6.0
                        Denegacion de servicio en windos NT/2000/XP. Servicio
                        Web Calendaring.

OpenSSH
                        Troyano en distribuciones espureas. Alguien se divirtio
                        a modificar los archivos openssh-3.4pl.tar.gz,
                        openssh-3.4.tgz, openssh-3.2.2pl.tar.gz e introdujo un
                        trayano. El proceso de firma no sirvio para nada.

Eudora 5.x (Qualcomm)
                        Desbordamiento de buffer en una construccion MIME
```

```
                        multiparte.

Macromedia Flash Player de Macromedia
                        Muestra informacion vital a webmaster malicioso.

Apache 2.0 anteriores a versiones 2.0.40
                        Afecta a sistemas no Unix. Muestra informacion vital.

OpenSSL
                        Desbordamiento de buffer.

Cisco CSS de la serie 11000
                        Falta de seguridad en acceso a la administracion via
                        web.

Oracle 9i SQL*NET
                        Vulnerables a ataques Cros-Site Scripting.

ToolTalk (en entorno CDE de Unix)
                        Denegacion de servicio y ejecucion de codigo arbitrario.

XINETD (Linux)
                        Posibilidad de matar procesos.

OpenBSD
                        Bloqueo de sistema. Sobreescribir memoria. Ejecucion
                        de codigo.

WebEasymail v.3.4.2.2
                        Denegacion de servicio.

Protocolo SMB de Windows
                        Desbordamiento de buffer. Denegacion de servicio.
                        Ejecucion de codigo arbitrario.

Raptor Firewall 6.5.x (Symantec)
                        El corta fuegos permite acceder al sistema protegido.

Microsoft Content Management Server 2001
                        Desbordamiento de buffer. Acceso a informacion
                        restringida. Ejecucion de codigo arbitrario.

Control ActiveX (Certificate Enrollment Control)
                        Eliminacion de los certificados diitales almacenados.

Webmin 0.92 y 0.921
                        Ejecucion de codigo arbitrario.

mIRC 6.03
                        Desbordamiento de buffer.

Facto System CMS
                        Inyeccion de instrucciones SQL.

Microsoft Visual FoxPro 6.0
                        Lanzamiento remoto de una aplicacion Visual a traves de
                        una pagina web o de un correo HTML.

Cisco VPN 3000
                        Autentificacion en IPSEC, vulnerabilidad en el cliente
                        Windows PPTP...
```

```
PGP Corporate Desktop 7.1.1
                        Desbordamiento de buffer.

Zmerge (Lotus Notes/Domino)
                        Acceso como administrador a todos los usuarios.

Tru64 (Unix de Compaq)
                        Denegacion de servicio, desbordamiento de buffer.

PostgreSQL 7.2.2
                        Ejecucion de codigo arbitrario.

OpenSSL de Apache
                        Conversion de sistema en zombi.
```

ANALISIS CASUAL

Por mis manos han pasado 72 referencias (sino me he equivacado al sumar) repartidas de la forma siguiente.

Productos Windows	20 acontecimientos
Apache	4
Oracle	3
Otros	49 (si no me he equivocado al restar)

Como puede ver un observador casual, Microsoft gana en las encuestas y no precisamente por minima ventaja. Pero no nos precipitemos ni hagamos juicios demasiado superficiales. Es cierto que los productos de windows salen en todos los numeros y que cuando un producto multi-sistema-operativo se ve afectado por alguna vulnerabilidad, las consecuencias son normalmente mas graves en windows que en otro tipo de sistemas operativos, pero tambien es cierto que hay mucha gente buscando defectos en Excel y probablemente no hay nadie buscandole las cosquillas al StarOffice. El motivo es obvio. Si encuentras un bug en el Word, las consecuencias son inmediatas :

- Tienes una publicidad enorme (si quieres anunciar tu hallazgo).
- Tienes una cantidad apabullante de posibles victimas (si quieres guardar el secreto para un selecto grupo de amigos).

En cambio un error en PsPice, encontrara un eco minimo (tirando a nulo) y las posibilidades que los podais explotar para atacar el server tras del cual llevas varios meses, son practicamente nulas.

COMENTARIOS PROPIOS

Lo que voy a escribir forma parte tan solo de mi personal punto de vista, asi que haced el favor de no atacar a SET si alguien esta en total desacuerdo con las letras que a continuacion van a formar ciertas frases levemente coherentes.

No creo que los productos Windows sean particularmente malos en cuanto a seguridad, creo que son simplemente un reflejo de la mediocridad de nuestra cultura. En nuestra civilizacion occidental, no hay nadie capaz de decir no a un minimo beneficio y lo malo es que este interes puede ser tanto monetario como simplemente de prestigio. Pocos escapan a la satisfaccion de ver aparecer su nombre en los titulos de un programa y comprobar que este se va replicando a lo largo de la red, si encima te pagan por ello o hay posibilidades de conseguir una promocion en tu deplorable empresa, todo arrastra a sacar productos mal chequeados.

Hubo otras civilizaciones y culturas, en las cuales se trabajaba por el placer de realizar obras, artefactos o disenyos que eran perfectos en si y por si mismos, que conseguian gracias a su perfeccion que alguien retribuyera su trabajo sea de forma transitoria (mecenazgo), permanente (el sistema esclavista romano, funcionaba en algunas zonas del imperio de esa forma) o contractual (los sistemas gremiales fueron consecuencia de este punto de vista).

Solo la avaricia a corto plazo, puede explicar que productos tales como Kazaa, salgan a la red con majaderias del tipo como que no se sepa exactamente donde se encuentran los ficheros que se van a compartir. Que no se advierta claramente que un leve error en la configuracion del programa, puede provocar que todo el disco de su ordenador, esta disponible a la vista de cualquier zangano que se pasee por la red. Este es un caso claro en el cual para evitar que el programa no funcione ’a la primera’ se pierde todo control sobre la seguridad. O sea que en el fondo se esconde informacion al usuario, que solo es consciente que el sistema funciona a maravilla para el objetivo de compartir musica, pero que es un petardo en cuanto a disimular el numero de telefono de tu ultima/o amante.

Solo este tipo de comportamiento irresponsable, permite que salgan al mercado presuntos corta-fuegos (Raptor Firewall 6.5.x (Symantec)) que permiten ver lo que se encuentra detras de el. Este caso es mas grave si cabe, ya que el usuario cree encontrarse protegido, cuando lo unico que hace es llamar la atencion sobre el, ya que es mas facil buscar en la red quien emplea este o aquel corta-fuegos que buscar a saco quien te va a deja entrar por despistado.

Las conclusiones particulares de tan singular forma de pensar (la mia), son que:

- Procuro instalarme programas un poco oscuros. No para evitar que el amigo Gates se llene el bolsillo sino para evitar ser blanco de algun gusano disenyado para la ultima version de Excel.

- Huyo de cortafuegos locales (prefiero pasar desapercibido), ademas todos sabemos que por cada error de hardware, existen mil de software, o sea que los cortafuegos en version hardware y pensandoselo mucho.

- Intento no instalar cosas inutiles.

En general me da lo mismo que Bill Gates sea el hombre mas rico del mundo. Si lo es, se debe simplemente a la mediocridad del resto de humanos y de la falta de criterio propio que normalmente aqueja al usuario medio de cualquier artilugio que se encuentra en este mundo (incluida le red). Menos ataques infundados o mal construidos contra Microsoft y similares. Si hay algo que no nos gusta, pues intentemos hacer cosas mejores. Si no somos capaces, tampoco es cuestion de cortarse las venas en la banyera, siempre podemos ayudar a los que si tienen las habilidades necesarias y maneras hay muchas. Citemos algunas:

- La primera, mas obvia, pero la menos seguida, es buscar algun substituto al programa molesto. (cuanta gente se queja de algo, pero no busca alternativas!)

- Si lo encuentras, no te quedes clavado a la primera dificultad.

- Intenta reproducir los bugs.

- Informa de ellos al creador del programa.

- Se razonable.

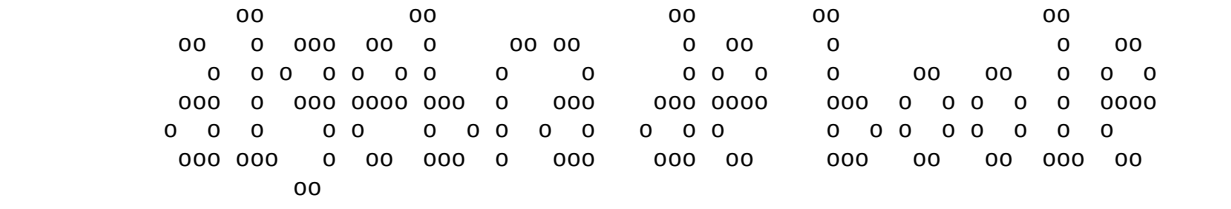
Solo es una corta reflexion.

madfran@nym.alias.net

EOF

```
-[ 0x09 ]--------------------------------------------------------------
-[ Analisis Booleano]--------------------------------------------------
-[ by Aristoteles ]-----------------------------------------------SET-26--
```

Este articulo es una base bastante completa para comenzar a adentrarse en la criptologia. No se trata de mostrar direcciones maravillosas ni trucos infalibles, es solo informacion basica,... dura informacion que solo os va a servir para algo en el caso de que posteriormente vosotros aporteis algun esfuerzo de desarrollo y ,.... compartais vuestro trabajo con el resto del mundo.



IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIlIlIllIlllIIlIIIllIlIIllll

para Angela, primera y ultima. gracias por todo lo que me has dado

Advertencia: Este texto contiene algunos caracteres extendidos que se muestran correctamente en la pagina 437 de MS-DOS. Ha sido necesario usarlos. La lista completa es:

"î" pertenencia:

```
  xxx
 xx
xx
xxxxx
xx
 xx
  xxx
```

"¤" letra enye minuscula:

```
    xxxx
    xxx
    xx
    xx
```

"í" conjunto vacio:

```
   x
  xxx
 x x x
 x x x
  xxx
  x
```

"": diferencia simetrica:

```
   x
  x x
 x   x
 xxxxx
```

"ª" negacion de una proposicion:

```
xxxxx
    x
```

"ð" equivalencia:

```
xxxxxx
xxxxxx
xxxxxx
```

(no es extendido, es DEL [127d])

Para establecer la pagina 437 en MS-DOS:

```
mode con cp prepare=((437) %windir%\command\ega.cpi)
mode con cp select=437
```

INDICE:

El algebra de G. Boole se puede aplicar a distintos campos:

   - operaciones binarias a nivel de bits
   - logica de proposiciones
   - algebra de conjuntos (y probabilidad)

OPERACIONES:

   Se definiran operaciones sobre uno y dos operandos cuyo resultado dependa
   de los operandos. Tambien se explicaran los resultados que no dependan de
   los operandos (resultados independientes).

   OPERACIONES SOBRE UN OPERANDO:

      Con un operando, podemos obtener cuatro resultados distintos, pero solo
      dos de ellos son operaciones que dependen del operando: identidad y not.

Los otros dos resultados no dependen del operando, y no seran tratados como operaciones, sino como distintos valores que podemos obtener. Son: anulacion y totalidad.

ANULACION:

Devuelve el valor nulo. El valor nulo es en cada caso:

bitwise: El valor nulo es el numero cero, se representa por: 0. En lenguajes de programacion indica el valor 'falso'. Todos los bits del campo son 0.

logica: El valor nulo es una asercion falsa (una proposicion siempre falsa, tambien llamada contradiccion o falacia).
Ejemplo: P y no P, "Soy humano Y NO soy humano"

conjuntos: Se llama conjunto vacio el conjunto que no contiene ningun elemento. Esta incluido en cualquier conjunto (por la definicion de inclusion). Se representa por: í

TOTALIDAD:

El valor total depende del tama¤o con que lo hayamos definido. En cada caso es:

bitwise: El valor total es un numero de todo unos, dependiendo del tama¤o que tenga el campo en que estemos trabajando; por ejemplo, en 16 bits el valor total es 65535d. Se representa por -1, que es el valor que toma un numero de todo unos en la aritmetica de complemento a dos. En lenguajes de programacion indica 'verdadero' (aunque en general, cualquier numero distinto de 0 es tratado como verdadero).

logica: El valor total es una asercion verdadera (una proposicion siempre verdadera, o tautologia).
Ejemplo: P o no P, "Estoy muerto O estoy vivo"

conjuntos: El valor total es el conjunto total, que contiene a todos los demas conjuntos. Es complementario del conjunto vacio. Se suele representar por E.

IDENTIDAD:

Esta operacion actua sobre un operando. Devuelve el propio operando.

bitwise: Id x = x
Ejemplo: Id 123d = 123d

logica: (Id P) <=> P
(la identidad de P es cierta si y solo si P es cierta)

conjuntos: Id A = A
Ejemplo: x î Id A <=> x î A

NOT:

```
   ----

   Esta operacion actua sobre un unico operando. Devuelve el complementario
   del operando; depende, pues, del valor total. En cada caso:

   bitwise: Modifica el valor de cada bit. Si un bit esta establecido, lo
            pone a 0 y si esta a 0 lo pone a 1. Su resultado depende del
            tama¤o del campo en que trabajemos.
            Ejemplos: not 5 (en 4 bits) = 10d
                      not 5 (en 8 bits) = not 101b (en 8 bits) = 11111010b
                      = 128d+64d+32d+16d+8+2 = 250d
            Si empleamos numeros con signo usando aritmetica de complemento
            a 2, entonces: not a = -a-1 (cualquiera que sea el tama¤o
            total, puesto que el cambio de signo es una operacion que ya
            depende del tama¤o total).
            Ejemplo: not 5 (en 8 bits con signo) = -6
                     not 5 (en 32d bits con signo) = -6

   logica: Opera sobre una unica asercion. Si la asercion es verdadera, el
           resultado es falso. Si la asercion es falsa, el resultado es
           verdadero.
           NO P es verdadera si y solo si P es falsa,
           NO P es falsa si y solo si P es verdadera.
           Ejemplo: "Estoy vivo Y estoy muerto" es falsa,
                    "NO (estoy vivo Y estoy muerto)" es verdadera, ya que
                    por las leyes de De Morgan, es equivalente a:
                    "NO estoy vivo O NO estoy muerto" <=>
                    "Estoy muerto O estoy vivo"... es verdadera.

   conjuntos: El complementario de un conjunto A es el conjunto de los
              elementos de E que no pertenecen a A. El complementario se
              representa por: C  A  o tambien: A'
                              E


OPERACIONES SOBRE DOS OPERANDOS:
--------------------------------

   Sobre dos operandos podemos obtener 16 resultados, de los cuales:
      - dos no dependen de ningun operando: anulacion y totalidad
      - dos dependen solo del primer operando: 'identidad del primer
        operando' y 'complementario del primer operando'
      - dos dependen solo del segundo operando: 'identidad del segundo
        operando' y 'complementario del segundo operando'
      - diez dependen de ambos operandos: and, or, xor, 'diferencia del
        primero y el segundo', 'diferencia del segundo y el primero', nand,
        nor, xnor, 'primero implica segundo', y 'segundo implica primero'.


   ANULACION:
   ----------

   Recibe dos operandos, y devuelve el valor nulo, segun cada caso. Este
   resultado no depende de ninguno de sus dos operandos, y es independiente
   del valor total.


   TOTALIDAD:
   ----------

   Recibe dos operandos, y devuelve el valor total segun cada caso. Este
   resultado no depende de ninguno de sus dos operandos. Si depende del
```

valor total que hayamos definido.

IDENTIDAD DEL PRIMERO:

Toma dos operandos. Devuelve verdadero si y solo si el primer operando es verdadero. El resultado es independiente del segundo operando.

bitwise: Compara dos numeros bit a bit. Devuelve 1 si y solo si el bit del primer operando es 1. No tiene en cuenta el segundo numero.
Ejemplo: 127d * 7 = 127d
(donde "*" denota la identidad del primer numero)

logica: El resultado sera verdadero si y solo si la primera asercion es verdadera. Es independiente de la segunda asercion.
Ejemplo: (P * Q) <=> P
("*" denota la identidad de la primera asercion)

conjuntos: El resultado es el primer conjunto (primer operando), y es independiente del segundo conjunto.
Ejemplo: xîA*B <=> xîA
("*" denota la identidad del primer conjunto)

COMPLEMENTARIO DEL PRIMERO:

Recibe dos operandos, y devuelve el complementario del primero; es independiente del segundo operando. El resultado depende del valor total.

bitwise: Compara los dos operandos bit a bit. Devuelve 0 si el bit del primero es 1, y devuelve 1 si el bit del primero es 0 (es independiente del segundo operando). Su resultado depende del tama¤o del campo en que trabajemos.
Ejemplo: 15d * 5 (en 5 bits) = 10000b = -16
("*" denota la operacion ’not primer operando’)

logica: La operacion devuelve verdadero si y solo si la primera asercion es falsa (es independiente de la segunda).
Ejemplo: P * Q <=> no P
("*" denota ’complementaria de la primera asercion’)

conjuntos: El resultado es el complementario del primer conjunto. Es independiente del segundo conjunto. Su resultado depende del conjunto total.
Ejemplo: A*B=A’
("*" denota el complementario del primer conjunto)

IDENTIDAD DEL SEGUNDO:

(Ver identidad del primero)

COMPLEMENTARIO DEL SEGUNDO:

(Ver complementario del primero)

Se acabaron las operaciones absurdas (al menos habia que citarlas).

AND:

Trabaja con dos operandos. Devuelve verdadero si y solo si los dos operandos son verdaderos (falso en el resto de los casos). Por tanto, su resultado no depende del tama¤o del valor total.

bitwise: Compara bit a bit, devolviendo un bit a 1 si y solo si los dos bits son 1. Se conoce tambien con el nombre de producto logico.
Ejemplo: 1001b and 1100b = 1000b

logica: La asercion resultante es verdadera si y solo si las dos aserciones son verdaderas. Se llama conjuncion de proposiciones.
P Y Q es verdadera si y solo si P es verdadera y Q es verdadera
Ejemplo: "Existo Y soy humano" <=> "Soy humano"
^
por: "Soy humano" => "Existo"

conjuntos: La interseccion de dos conjuntos es el conjunto de los elementos que pertenecen a la vez a ambos conjuntos. Si la interseccion de los conjuntos es el conjunto vacio, se dice que son conjuntos disjuntos entre si (si no, decimos que los conjuntos se encuentran o se cortan).
AnB = { x | xîA Y xîB }

OR:

Recibe dos operandos. Su resultado es verdadero si y solo si al menos uno de los operandos es verdadero. No depende del valor total. Es un 'o' con sentido inclusivo (un operando no excluye al otro).

bitwise: Trabaja bit a bit. Devuelve 1 si y solo si al menos uno de los dos bits vale 1. Tambien conocido como suma logica.
Ejemplo: 0101b or 1001b = 1101b

logica: El resultado es verdadero si y solo si al menos una de las dos aserciones es verdadera. Es un O inclusivo (pueden ser ambas verdaderas). Se llama disyuncion/disjuncion de proposiciones. En el lenguaje cotidiano, a veces se utiliza: "y/o".
P o Q <=> P es verdadera O Q es verdadera

conjuntos: La union (o reunion) de dos conjuntos es el conjunto de los elementos de ambos conjuntos.
AuB = { x | xîA O xîB }

XOR:

Recibe dos operandos, y devuelve verdadero si y solo si un unico operando es verdadero (y el otro es falso). Un operando excluye al otro, y para que el resultado sea verdadero, los operandos deben ser distintos. Es un 'o' con sentido exclusivo. Su resultado no depende del valor total. XOR es una doble diferencia logica (ver diferencia logica).

bitwise: Opera bit a bit, y devuelve verdadero si y solo si un operando

es 1 y el otro es 0. Se llama tambien suma logica exclusiva.
Ejemplo: 1100b xor 0110b = 1010b

logica: La asercion resultante es verdadera si y solo si una unica asercion es cierta (y la otra falsa). Una asercion excluye a la otra, y no pueden ser ambas verdaderas o ambas falsas.
P O BIEN Q <=> (P es cierta Y Q es falsa) O
(P es falsa Y Q es cierta)
Ejemplo: "Soy hombre O BIEN soy mujer" es una asercion cierta (asumiendo que no hay puntos medios).

conjuntos: Se llama diferencia simetrica de dos conjuntos al conjunto formado por los elementos de ambos conjuntos que no pertenecen a los dos conjuntos al mismo tiempo.
AB = { x | xîA Y xîB Y xî(AnB)' }

DIFERENCIA LOGICA DEL PRIMERO Y EL SEGUNDO:

Es una operacion sobre dos operandos. Su resultado es verdadero si y solo si el primer operando es verdadero y el segundo es falso. Por lo tanto, su resultado es independiente del valor total. Esta operacion no es asociativa ni conmutativa.

bitwise: Trabaja bit a bit. Devuelve 1 si y solo si el primer operando es 1 y el segundo 0. Se llama diferencia logica.
Ejemplo: 0101b - 1100b = 0001b
("-" denota la diferencia logica del 1o y el 2o)

logica: La asercion resultado es verdadera si y solo si la primera asercion es verdadera y la segunda falsa.
P - Q <=> P Y NO Q
Ejemplo: "(x es primo) - (x es impar)" <=>
"x es primo" Y "x es par" <=> "x es 2"
("-" denota la diferencia logica del 1o y el 2o)

conjuntos: La diferencia de dos conjuntos es el conjunto formado por los elementos pertenecientes al primer conjunto y no pertenecientes al segundo conjunto.
A-B = { x | xîA Y xîB' }

DIFERENCIA LOGICA DEL SEGUNDO Y EL PRIMERO:

Esta operacion es la diferencia logica en el otro sentido, obteniendose resultados diferentes (ver diferencia logica del primero y el segundo). Tampoco cumple la propiedad asociativa ni la conmutativa (si fuese conmutativa, las dos diferencias serian la misma operacion).

Ahora se explicaran las complementarias de estas cinco operaciones.

NAND:

Es la operacion complementaria de AND (el resultado de AND es negado). Recibe dos operandos, y devuelve verdadero si y solo si al menos uno de los operandos es falso. Su resultado depende del valor total. Esta operacion no se suele usar.

```
bitwise: Compara bit a bit. Devuelve 1 si y solo si al menos uno de los
         operandos es 0 (devuelve 0 si ambos son 1).
         Ejemplo: 0011b nand 0110b (en 4 bits) = 1101b

logica: Devuelve una asercion verdadera si y solo si al menos una de las
        aserciones es falsa.
        P NAND Q <=> NO (P Y Q) <=> (NO P) O NO Q (leyes de De Morgan)

conjuntos: El conjunto resultante de esta operacion es el complementario
           de la interserccion de los dos conjuntos operandos.
           An'B = (AnB)' = { x | xî(AnB)' } = { x | xîA' O xîB' }= A'uB'
           ("n'" denota el complementario de la interseccion)


NOR:
----

Es la operacion complementaria de OR (el resultado de OR es negado).
Trabaja con dos operandos. Devuelve verdadero si y solo si los dos
operandos son falsos, por tanto, su resultado depende del valor total.
Esta operacion tampoco se suele usar.

bitwise: Trabaja bit a bit. Devuelve un bit a 1 si y solo si ambos
         operandos son 0 (devuelve 0 en el resto de casos).
         Ejemplo: 0101b nor 0011b (en 4 bits) = 1000b

logica: La asercion resultante es cierta si y solo si ambas aserciones
        son falsas.
        P NOR Q <=> NO (P O Q) <=> (NO P) Y (NO Q)

conjuntos: El conjunto resultante es el complementario de la union de
           los conjuntos operandos.
           Au'B = (AuB)' = { x | xî(AuB)' } = { x | xîA' Y xîB' }= A'nB'
           ("u'" denota el complementario de la union de conjuntos)


XNOR / EQUIVALENCIA:
--------------------

Esta operacion es muy importante. Se trata de la negacion del resultado
de XOR (es su operacion complementaria). Su resultado es verdadero si y
solo si ambos resultados son verdaderos o ambos resultados son falsos.
Por esta definicion, su resultado depende del valor total. Es una
equivalencia, o implicacion en los dos sentidos.

bitwise: Compara bit a bit. Devuelve 1 si y solo si los dos bits
         operandos son iguales (que sean ambos 1 o que sean ambos 0).
         A nivel de bits esta operacion se llama xnor.
         Ejemplo: 0011b xnor 1001b (en 4 bits) = 0101b

logica: El resultado es una asercion verdadera si y solo si ambas
        aserciones son verdaderas o ambas aserciones son falsas. Se
        trata de la equivalencia tan usada en matematicas (tambien
        llamada doble implicacion o condicional).

        (P <=> Q) <=> (P => Q) Y (Q => P)

        'P <=> Q' se lee:
           P es condicion necesaria y suficiente de Q
           P si y solo si Q
           P es equivalente logico de Q
```

Ejemplo: "(x + 1 = 1) <=> (x = 0)" es una asercion verdadera.

conjuntos: El resultado de operar dos conjuntos es el conjunto de los elementos que pertenecen a la vez a ambos conjuntos o que no pertenecen a ninguno. Depende del conjunto total.
xî(A<=>B) <=> (xîAnB O xî(AuB)')
(en este caso, "<=>" denota la operacion 'equivalencia entre conjuntos', aunque nunca se utiliza [se compone con las operaciones basicas not, and y or]).

IMPLICACION PRIMERO => SEGUNDO:

Es la operacion complementaria de la diferencia logica del primero y el segundo. Devuelve verdadero si y solo si: el primer operando es cierto y el segundo tambien, o si el primero es falso. Esta es la definicion de implicacion, una operacion que depende del tama¤o del valor total.

bitwise: No se suele utilizar directamente. Compara a nivel de bits, y devuelve 1 cuando el primer bit es 0, o cuando el primer bit es 1 y el segundo es 1. Como ya he dicho, depende del tama¤o total del campo en que trabajemos.
Ejemplo: (1100b => 0110b) (en 8 bits) = 11110111b
("=>" denota la operacion implicacion a nivel de bits)

logica: La asercion resultante es cierta si y solo si la primera asercion es cierta y la segunda tambien, o si la primera asercion es falsa. La implicacion simple tambien se utiliza mucho en demostraciones (sobretodo en demostraciones de un solo sentido).

(P => Q) <=> [(P Y Q) O NO P] <=> (NO P) O Q

'P => Q' se lee:
P es condicion suficiente de Q
Q es condicion necesaria de P
Si P, entonces Q
P solo si Q
Q si P
P implica Q
P entra¤a Q

La proposicion P recibe el nombre de hipotesis, y Q tesis o conclusion. En una demostracion es posible que, al tomar la hipotesis como falsa, lleguemos a una contradiccion, por lo que la proposicion quedaria demostrada (por el principio del medio excluido).

Ejemplo: "Si tengo pies, entonces tengo piernas" es una asercion verdadera, y equivalente a: "NO tengo pies O tengo piernas". Es posible que este ultimo enunciado te confunda, lo veras mas claro si analizas los casos:

no tener pies ni piernas
no tener pies y tener piernas
tener pies y no tener piernas (imposible)
tener pies y piernas

conjuntos: El resultado de esta operacion es el conjunto de los elementos del conjunto total que no pertenecen al primer

```
                conjunto o que pertenecen al segundo. El resultado depende
                del conjunto total.
                xî(A=>B) <=> (xîA' O xîB) <=> [(xîA O xîA') Y (xîA' O xîB)]
                <=> [xîA' O (xîA Y xîB)]
                 ^
                 por las propiedades distributivas
                ("=>" denota la implicacion entre conjuntos)
```

IMPLICACION SEGUNDO => PRIMERO:

Se trata de la implicacion en el otro sentido (primero <= segundo). (Ver implicacion primero => segundo).

OPERACIONES SOBRE MAS DE DOS OPERANDOS:

Sobre n operandos se pueden obtener 4^n resultados distintos. Habra algunos que no dependan de ningun operando, otras que dependan de algunos operandos, y otros que dependan de todos los operandos. Todas las operaciones sobre mas de dos operandos pueden ser compuestas mediante las operaciones ya descritas. Shannon lo demostro, y tambien probo que todas las operaciones pueden ser compuestas mediante {and, not}, {or, not}, etc

TABLA DE SIGNOS:

Los distintos signos que se suelen usar para indicar las operaciones son:

operacion:	bitwise			logica				conjuntos	
	_							_	
not	A	~A	not A	no P	!P	ªP	~P	A	A'
and	A*B	A&B	A and B	P y Q	P&&Q	P/\Q		AnB	
or	A+B	A|B	A or B	P o Q	P||Q	P\/Q		AuB	
xor	A(+)B	A^B	A xor B	P o bien Q				AB	
dif. logica	A-B							A-B	
nand			A nand B						
xnor/equival.			A xnor B	P <=> Q					
implicacion				P => Q					

No se recomienda usar la notacion de C o de otro lenguaje para evitar confusiones. El valor total y el valor nulo se suelen representar:

bitwise	logica	conjuntos
0	FALSO	í
-1	VERDADERO	E

NOMBRES DE LAS OPERACIONES:

Cada operacion puede tener un nombre distinto segun el campo en que se utilice:

nivel de bits	logica	conjuntos

not	negacion	complementario
and/producto logico	conjuncion	interseccion
or/suma logica	disyuncion	union/reunion
xor/suma logica exclusiva	disyuncion exclusiva???	diferencia simetrica
diferencia logica	??? (P y no Q)	diferencia
nand	??? (no (P y Q))	??? ((AnB)')
nor	??? (no (P o Q))	??? ((AuB)')
xnor	equivalencia	??? ((AB)')
??? (not dif. log.)	implicacion	??? ((A-B)')

PROPIEDADES:

A continuacion se describen las propiedades de las operaciones descritas. No se demuestra ninguna, porque eso lo puede hacer el lector. La forma mas rapida es demostrarlas para todas las combinaciones posibles de operandos y los resultados que producen (puesto que estan definidas sobre conjuntos finitos).

Para describir las operaciones se empleara notacion de nivel de bits, con algunas extensiones (ver tabla de signos). Se utilizara "=>" para la implicacion y "<=>" o "xnor" para la equivalencia. Se utilizara A' para indicar el complementario de A.

Evidentemente, las propiedades son aplicables a los tres campos (nivel de bits, logica, y conjuntos). La igualdad debe ser sustituida solo en logica por la equivalencia ("<=>").

ASOCIATIVA:

Definicion: Para cualesquiera x, y, z: x * (y * z) = (x * y) * z
("*" denota la operacion)

Cumplen la propiedad asociativa: anulacion, and, identidad del primero, identidad del segundo, xor, or, nor, xnor, complementario del segundo, complementario del primero, nand, y totalidad.

A * (B * C) = (A * B) * C = A * B * C (and)

A (+) (B (+) C) = (A (+) B) (+) C = A (+) B (+) C (xor)

A + (B + C) = (A + B) + C = A + B + C (or)

CONMUTATIVA:

Definicion: Para cualesquiera x, y: x * y = y * x

Cumplen la conmutativa: anulacion, and, xor, or, nor, xnor, nand, y totalidad.

A * B = B * A (and)

A (+) B = B (+) A (xor)

A + B = B + A (or)

IDEMPOTENCIA: (o fridegidez)

Definicion: Para todo x: x * x = x
("*" denota la operacion idempotente)

Cumplen la idempotencia las operaciones: and, identidad del primero, identidad del segundo, y or.

A * A = A (and)

A + A = A (or)

ELEMENTO NEUTRO:

Definicion: Existe un elemento e tal que para todo x: e * x = x * e = x
Es posible que exista elemento neutro sin que se de la propiedad conmutativa, aunque en estas operaciones no ocurre en ningun caso.

Tienen elemento neutro: and, xor, or, xnor.

El elemento neutro de and y xnor es el valor total (-1 en nivel de bits):

A * -1 = -1 * A = A (and)

A xnor -1 = -1 xnor A = A (xnor)

El elemento neutro de xor y or es el valor nulo (0 a nivel de bits):

A (+) 0 = 0 (+) A = A (xor)

A + 0 = 0 + A = A (or)

ELEMENTO INVERSO:

Definicion: Para todo x existe un y tal que: x * y = y * x = e
En otras palabras, todo elemento tiene simetrico. Tambien puede existir elemento neutro sin que se de la propiedad conmutativa para todos los elementos, aunque tampoco ocurre con ninguna operacion de las explicadas. Si es necesario que exista elemento neutro.

Tienen elemento inverso la operaciones: xor y xnor.

El elemento inverso de estas operaciones es el propio operado:

A (+) A = 0 (xor)

```
   A xnor A = -1   (xnor)


DISTRIBUTIVA:
-------------

Existen dos propiedades distributivas: por la izquierda y por la derecha,
no es necesario que se de la propiedad conmutativa para que se cumplan
ambas, aunque si se da, entonces se cumplen las dos.

Definicion: por la izquierda:
            Para cualesquiera x, y, z: x * (y (*) z) = (x * y) (*) (x * z)
            ("*" denota una operacion, y "(*)" denota otra)

            por la derecha:
            Para cualesquiera x, y, z: (y (*) z) * x = (y * x) (*) (z * x)

Se lee: "la operacion * es distributiva por la izquierda o por la derecha
en relacion a la operacion (*)".

Cumplen la propiedad distributiva solo por la izquierda los pares de
operaciones siguientes:

   (diferencia segundo - primero, anulacion)
   (diferencia segundo - primero, and)
   (diferencia segundo - primero, diferencia primero - segundo)
   (diferencia segundo - primero, diferencia segundo - primero)
   (diferencia segundo - primero, xor)
   (diferencia segundo - primero, or)
   (identidad segundo, anulacion)
   (identidad segundo, diferencia primero - segundo)
   (identidad segundo, diferencia segundo - primero)
   (identidad segundo, xor)
   (identidad segundo, nor)
   (identidad segundo, xnor)
   (identidad segundo, complementario segundo)
   (identidad segundo, implicacion segundo => primero)
   (identidad segundo, complementario primero)
   (identidad segundo, implicacion primero => segundo)
   (identidad segundo, nand)
   (identidad segundo, totalidad)
   (complementario segundo, complementario segundo)
   (complementario segundo, complementario primero)
   (complementario primero, and)
   (complementario primero, or)
   (implicacion primero => segundo, and)
   (implicacion primero => segundo, or)
   (implicacion primero => segundo, xnor)
   (implicacion primero => segundo, implicacion segundo => primero)
   (implicacion primero => segundo, implicacion primero => segundo)
   (implicacion primero => segundo, totalidad)

Cumplen la propiedad distributiva solo por la derecha los siguientes pares:

   (diferencia primero - segundo, anulacion)
   (diferencia primero - segundo, and)
   (diferencia primero - segundo, diferencia primero - segundo)
   (diferencia primero - segundo, diferencia segundo - primero)
   (diferencia primero - segundo, xor)
   (diferencia primero - segundo, or)
   (identidad primero, anulacion)
```

```
(identidad primero, diferencia primero - segundo)
(identidad primero, diferencia segundo - primero)
(identidad primero, xor)
(identidad primero, nor)
(identidad primero, xnor)
(identidad primero, complementario segundo)
(identidad primero, implicacion segundo => primero)
(identidad primero, complementario primero)
(identidad primero, implicacion primero => segundo)
(identidad primero, nand)
(identidad primero, totalidad)
(complementario segundo, and)
(complementario segundo, or)
(implicacion segundo => primero, and)
(implicacion segundo => primero, or)
(implicacion segundo => primero, xnor)
(implicacion segundo => primero, implicacion segundo => primero)
(implicacion segundo => primero, implicacion primero => segundo)
(implicacion segundo => primero, totalidad)
(complementario primero, complementario segundo)
(complementario primero, complementario primero)
```

Cumplen la propiedad distributiva (por la izquierda y por la derecha) los pares de operaciones:

```
(anulacion, anulacion)
(anulacion, and)
(anulacion, diferencia primero - segundo)
(anulacion, identidad primero)
(anulacion, diferencia segundo - primero)
(anulacion, identidad segundo)
(anulacion, xor)
(anulacion, or)
(and, anulacion)
(and, and)
(and, diferencia primero - segundo)
(and, identidad primero)
(and, diferencia segundo - primero)
(and, identidad segundo)
(and, xor)
(and, or)
(diferencia primero - segundo, identidad primero)
(diferencia primero - segundo, identidad segundo)
(identidad primero, and)
(identidad primero, identidad primero)
(identidad primero, identidad segundo)
(identidad primero, or)
(diferencia segundo - primero, identidad primero)
(diferencia segundo - primero, identidad segundo)
(identidad segundo, and)
(identidad segundo, identidad primero)
(identidad segundo, identidad segundo)
(identidad segundo, or)
(xor, identidad primero)
(xor, identidad segundo)
(xor, complementario segundo)
(xor, complementario primero)
(or, and)
(or, identidad primero)
(or, identidad segundo)
(or, or)
(or, xnor)
```

```
   (or, implicacion segundo => primero)
   (or, implicacion primero => segundo)
   (or, totalidad)
   (nor, identidad primero)
   (nor, identidad segundo)
   (xnor, identidad primero)
   (xnor, identidad segundo)
   (xnor, complementario segundo)
   (xnor, complementario primero)
   (complementario segundo, identidad primero)
   (complementario segundo, identidad segundo)
   (implicacion segundo => primero, identidad primero)
   (implicacion segundo => primero, identidad segundo)
   (complementario primero, identidad primero)
   (complementario primero, identidad segundo)
   (implicacion primero => segundo, identidad primero)
   (implicacion primero => segundo, identidad segundo)
   (nand, identidad primero)
   (nand, identidad segundo)
   (totalidad, and)
   (totalidad, identidad primero)
   (totalidad, identidad segundo)
   (totalidad, or)
   (totalidad, xnor)
   (totalidad, implicacion segundo => primero)
   (totalidad, implicacion primero => segundo)
   (totalidad, totalidad)

Los 16 pares de operaciones no citados no cumplen ninguna. Si alguien
encuentra un error en esta lista, que me lo haga saber. He hecho la lista
con un programa, y es posible que por algun error de implementacion sea
incorrecta. Gracias.

Las mas importantes son:

   A * (B - C) = (A * B) - (A * C)         (and, dif. primero - segundo)
   (B - C) * A = (B * A) - (C * A)

   A * (B + C) = (A * B) + (A * C)         (and, or)
   (B + C) * A = (B * A) + (C * A)

   A * (B (+) C) = (A * B) (+) (A * C)     (and, xor)
   (B (+) C) * A = (B * A) (+) (C * A)

   A + (B * C) = (A + B) * (A + C)         (or, and)
   (B * C) + A = (B + A) * (C + A)

   A + (B => C) = ((A + B) => (A + C))     (or, implic. primero => segundo)
   (B => C) + A = ((B + A) => (C + A))

   A + (B <=> C) = ((A + B) <=> (A + C))   (or, equivalencia/xnor)
   (B <=> C) + A = ((B + A) <=> (C + A))

Observese que la suma logica es distributiva en relacion al producto
logico; esto no ocurre en la suma y el producto aritmeticos.


LEYES DE De Morgan:
-------------------

Definicion: Para cualesquiera x, y, se cumple: (x * y)' = x' (*) y'
            ("*" denota una operacion, y "(*)" denota otra)
```

Cumplen las leyes de De Morgan los siguientes pares de operaciones:

(anulacion, totalidad)
(and, or)
(diferencia primero - segundo, implicacion segundo => primero)
(identidad primero, identidad primero)
(diferencia segundo - primero, implicacion primero => segundo)
(identidad segundo, identidad segundo)
(xor, xnor)
(or, and)
(nor, nand)
(xnor, xor)
(complementario segundo, complementario segundo)
(implicacion segundo => primero, diferencia primero - segundo)
(complementario primero, complementario primero)
(implicacion primero => segundo, diferencia segundo - primero)
(nand, nor)
(totalidad, anulacion)

Las realmente importantes son:

(A * B)' = A' + B' (and, or)

(A - B)' = (A' <= B') (dif. prim. - seg., implic. seg. => prim.)

(A (+) B)' = (A' <=> B') (xor, equivalencia/xnor)

(A + B)' = A' * B' (or, and)

(A <=> B)' = A' (+) B' (equivalencia/xnor, xor)

(A => B)' = B' - A' (implic. prim. => seg., dif. seg. - prim.)
(perdon por el cambio, pero no hay mas simbolos)

LEYES DE ABSORCION:

Las leyes de absorcion se dan entre dos operaciones. Existen cuatro tipos de leyes de absorcion.

Definicion: por la izquierda-izquierda: (tiene que tener un nombre)
para cualesquiera x, y: x * (x (*) y) = x

por la izquierda-derecha:
para cualesquiera x, y: x * (y (*) x) = x

por la derecha-izquierda:
para cualesquiera x, y: (x (*) y) * x = x

por la derecha-derecha:
para cualesquiera x, y: (y (*) x) * x = x

Cumplen las leyes de absorcion solo por la izquierda-izquierda:

(diferencia primero - segundo, diferencia segundo - primero)
(diferencia primero - segundo, complementario primero)
(complementario segundo, complementario primero)
(implicacion segundo => primero, complementario primero)
(implicacion segundo => primero, implicacion primero => segundo)

```
Solo por la izquierda-derecha:

   (diferencia primero - segundo, diferencia primero - segundo)
   (diferencia primero - segundo, complementario segundo)
   (complementario segundo, complementario segundo)
   (implicacion segundo => primero, complementario segundo)
   (implicacion segundo => primero, implicacion segundo => primero)

Solo por la derecha-izquierda:

   (diferencia segundo - primero, diferencia segundo - primero)
   (diferencia segundo - primero, complementario primero)
   (complementario primero, complementario primero)
   (implicacion primero => segundo, complementario primero)
   (implicacion primero => segundo, implicacion primero => segundo)

Solo por la derecha-derecha:

   (diferencia segundo - primero, diferencia primero - segundo)
   (diferencia segundo - primero, complementario segundo)
   (complementario primero, complementario segundo)
   (implicacion primero => segundo, complementario segundo)
   (implicacion primero => segundo, implicacion segundo => primero)

Solo por la izquierda-izquierda y por la izquierda-derecha:

   (diferencia primero - segundo, anulacion)
   (diferencia primero - segundo, nor)
   (identidad primero, anulacion)
   (identidad primero, and)
   (identidad primero, diferencia primero - segundo)
   (identidad primero, diferencia segundo - primero)
   (identidad primero, xor)
   (identidad primero, or)
   (identidad primero, nor)
   (identidad primero, xnor)
   (identidad primero, complementario segundo)
   (identidad primero, implicacion segundo => primero)
   (identidad primero, complementario primero)
   (identidad primero, implicacion primero => segundo)
   (identidad primero, nand)
   (identidad primero, totalidad)
   (implicacion segundo => primero, nand)
   (implicacion segundo => primero, totalidad)

Solo por la izquierda-izquierda y por la derecha-izquierda:

   (and, identidad primero)
   (and, implicacion segundo => primero)
   (or, diferencia primero - segundo)
   (or, identidad primero)

Solo por la izquierda-izquierda y por la derecha-derecha:

   [ninguna]

Solo por la izquierda-derecha y por la derecha-izquierda:

   [ninguna]

Solo por la izquierda-derecha y por la derecha-derecha:
```

```
   (and, identidad segundo)
   (and, implicacion primero => segundo)
   (or, diferencia segundo - primero)
   (or, identidad segundo)

Solo por la derecha-izquierda y por la derecha-derecha:

   (diferencia segundo - primero, anulacion)
   (diferencia segundo - primero, nor)
   (identidad segundo, anulacion)
   (identidad segundo, and)
   (identidad segundo, diferencia primero - segundo)
   (identidad segundo, diferencia segundo - primero)
   (identidad segundo, xor)
   (identidad segundo, or)
   (identidad segundo, nor)
   (identidad segundo, xnor)
   (identidad segundo, complementario segundo)
   (identidad segundo, implicacion segundo => primero)
   (identidad segundo, complementario primero)
   (identidad segundo, implicacion primero => segundo)
   (identidad segundo, nand)
   (identidad segundo, totalidad)
   (implicacion primero => segundo, nand)
   (implicacion primero => segundo, totalidad)

Solo por la izquierda-izquierda y por la izquierda-derecha y por la
derecha-izquierda:

   (identidad primero, identidad primero)

Solo por la izquierda-izquierda y por la izquierda-derecha y por la
derecha-derecha:

   (identidad primero, identidad segundo)

Solo por la izquierda-izquierda y por la derecha-izquierda y por la
derecha-derecha:

   (identidad segundo, identidad primero)

Solo por la izquierda-derecha y por la derecha-izquierda y por la
derecha-derecha:

   (identidad segundo, identidad segundo)

Cumplen las leyes de absorcion (las cuatro propiedades) los siguientes
pares de operaciones:

   (and, or)
   (and, totalidad)
   (xor, anulacion)
   (or, anulacion)
   (or, and)
   (xnor, totalidad)

Es posible que la lista contenga errores. Los pares no citados (182) no
cumplen ninguna propiedad. Estos ultimos pares de operaciones son los mas
importantes:

   A * (A + B) = A   (and, or)
   A * (B + A) = A
```

```
(A + B) * A = A
(B + A) * A = A

A + (A * B) = A   (or, and)
A + (B * A) = A
(A * B) + A = A
(B * A) + A = A
```

OTRAS PROPIEDADES:

Aqui solo se trataran las operaciones not, and, or, diferencia, y xor. Estas operaciones son todas conmutativas menos la diferencia, asi que no se indicaran todos los sentidos en las siguientes formulas. Se recuerda que 0 representa el valor nulo y -1 el valor total.

Propiedades del complementario:

```
0' = -1
-1' = 0

(A')' = A

A' = -1 - A

A * A' = 0

A + A' = -1

A - A' = A
A' - A = A'

A (+) A' = -1
```

Propiedades del valor nulo:

```
A * 0 = 0

A + 0 = A

A - 0 = A
0 - A = 0

A (+) 0 = A
```

Propiedades del valor total:

```
A * -1 = A

A + -1 = -1

A - -1 = 0
-1 - A = A'

A (+) -1 = A'
```

Propiedades que definen la diferencia y la suma exclusiva:

```
A - B = A * B' = A - (A * B)

A (+) B = (A + B) - (A * B) = (A - B) + (B - A)
```

PROPIEDADES DE LA IMPLICACION:

Estas propiedades son a lo que muchos reducen la logica. Son necesarias para demostraciones. Nota/ FALSO representa una contradiccion, VERDADERO representa una tautologia.

NO NO P <=> P (principio de no-contradiccion y del medio excluso)

(P <=> Q) <=> [(P => Q) Y (Q => P)]

[(P => Q) Y (Q => R)] <=> (P => R) (demostracion directa)

(P => Q) <=> (Q O NO P) <=> NO (P Y NO Q)

NO P <=> (P => FALSO)

P <=> (VERDADERO => P)

(P => Q) <=> [(P Y NO Q) => FALSO]

(P => Q) <=> (NO Q => NO P) (contrapositivo)

APEDICE: TABLA DE OPERACIONES:

OPERACIONES SOBRE UN SOLO OPERANDO:

NOP	LDP	TOT	NOMBRE
0	n	n	anulacion
1	s	n	identidad del operando
2	s	s	complementario del operando
3	n	s	totalidad

leyenda:
NOP: numero de operacion.
LDP: resultado linealmente dependiente del operando.
TOT: resultado dependiente del tama¤o total.

Nota sobre el numero de operacion:

En operaciones sobre un operando, el numero de operacion en un valor de 2 bits que identifica el resultado de la operacion para todos los posibles operandos (0 o 1). Ver la siguiente tabla:

NOP	0	1
0	0	0
1	0	1
2	1	0
3	1	1

la tabla muestra los resultados de la operacion para cada operando. los resultados de cada operacion indican el numero de la operacion, por ejemplo, la operacion 3 devuelve los resultados 1 y 1, el numero de 2 bits 11 es 3. mediante el numero de operacion se pueden conocer todas las propiedades de una operacion.

OPERACIONES SOBRE DOS OPERANDOS:

Recuerda que combinando estas operaciones o las de un solo operando es posible obtener cualquier resultado para cualesquiera que sean los operandos (se entiende para mas de dos operandos). Sobre n operandos se pueden definir 4^n operaciones.

NOP	LD1	LD2	TOT	ASO	CON	IDM	EEN	EEI	NOMBRE
0	n	n	n	s	s	n	n	n	anulacion
1	s	s	n	s	s	s	s -1	n	and
2	s	s	n	n	n	n	n	n	diferencia primero - segundo
3	s	n	n	s	n	s	n	n	identidad primero
4	s	s	n	n	n	n	n	n	diferencia segundo - primero
5	n	s	n	s	n	s	n	n	identidad segundo
6	s	s	n	s	s	n	s 0	s OP	xor
7	s	s	n	s	s	s	s 0	n	or
8	s	s	s	s	s	n	n	n	nor
9	s	s	s	s	s	n	s -1	s OP	xnor / equivalencia
10	n	s	s	s	n	n	n	n	complementario del segundo
11	s	s	s	n	n	n	n	n	implicacion segundo => primero
12	s	n	s	s	n	n	n	n	complementario del primero
13	s	s	s	n	n	n	n	n	implicacion primero => segundo
14	s	s	s	s	s	n	n	n	nand
15	n	n	s	s	s	n	n	n	totalidad

Leyenda:
- NOP: numero de operacion.
- LD1: linealmente dependiente del primer operando.
- LD2: linealmente dependiente del segundo operando.
- TOT: dependiente del tama¤o total.
- ASO: cumple la propiedad asociativa (para cualesquiera x, y, z, se cumple: x*(y*z)=(x*y)*z).
- CON: cumple la propiedad conmutativa (para cualesquiera x e y, se cumple: x*y=y*x).
- IDM: cumple la idempotencia (para todo x, x*x=x)
- EEN: existe elemento neutro (existe un elemento e tal que para todo elemento x, se cumple: e*x=x*e=x. se puede hablar de elemento neutro si no se de la conmutativa para todos los elementos). se indica tambien cual es el elemento neutro, -1 representa el valor total y 0 el valor nulo.
- EEI: exite elemento inverso (para todo x existe un y tal que: x*y=y*x=e). se indica cual es este elemento inverso en cada caso (OP indica el propio operando).

Sobre el numero de operacion:

Ocupa 4 bits, que corresponden a los distintos resultados de cada operacion con las 4 posibles combinaciones de operandos. Observese la siguiente tabla de resultados:

NOP	0,0	0,1	1,0	1,1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1
12	1	1	0	0
13	1	1	0	1
14	1	1	1	0

por ejemplo, la operacion xor, de numero 6, produce los siguientes resultados:

```
  0 xor 0 = 0
  0 xor 1 =  1
  1 xor 0 =   1
  1 xor 1 =    0
           ------
            0110 = 6 (numero de xor)
```

el numero de operacion define sus resultados, y, por tanto, sus propiedades, la dependencia de sus operandos, y la existencia de elementos neutro e inverso.

```
   15   1   1   1   1
```

Sobre las operaciones complementarias: Las 8 primeras operaciones de la tabla (de numeros 0..7) son las que no dependen del tama¤o total, las 8 ultimas (8..15) son sus complementarias, y si dependen del tama¤o total del campo. Dos operaciones cuyos numeros suman 15 son complementarias. La dependencia lineal de sus operadores y las propiedades asociativa y conmutativa son las mismas para operaciones complementarias. Las operaciones 1 y 7 (and y or) tienen elemento neutro, sin embargo, sus complementarias no.

OPERACIONES DISTRIBUTIVAS:

por la izquierda: para cualesquiera x, y, z: x*(y(*)z)=(x*y)(*)(x*z)
por la derecha: para cualesquiera x, y, z: (y(*)z)*x=(y*x)(*)(z*x)

Las siguientes listas indican las operaciones distributivas en un numero de 8 bits. Los 4 bits de mayor peso indican el numero de la primera operacion, y los 4 de menor peso el de la segunda operacion. La primera operacion es distributiva en relacion a la segunda. Los numeros estan indicados en hexadecimal para que sea mas facil la descodificacion.

Por la izquierda:

```
40 41 42 44 46 47 50 52 54 56 58 59 5A 5B
5C 5D 5E 5F AA AC C1 C7 D1 D7 D9 DB DD DF
```

Por la derecha:

```
20 21 22 24 26 27 30 32 34 36 38 39 3A 3B
3C 3D 3E 3F A1 A7 B1 B7 B9 BB BD BF CA CC
```

Ambas (propiedad distributiva):

```
00 01 02 03 04 05 06 07 10 11 12 13 14 15 16 17
23 25 31 33 35 37 43 45 51 53 55 57 63 65 6A 6C
71 73 75 77 79 7B 7D 7F 83 85 93 95 9A 9C A3 A5
B3 B5 C3 C5 D3 D5 E3 E5 F1 F3 F5 F7 F9 FB FD FF
```

leyes de De Morgan:

para cualesquiera x, y: (x*y)'=x'(*)y'

La siguiente lista incluye los pares de operaciones que cumplen las leyes de De Morgan. El formato es el mismo que el usado en las operaciones distributivas: los 4 bits de mayor peso indican la primera operacion, y los 4 bits de menor peso la segunda.

Cumplen las leyes de De Morgan:

```
0F 17 2B 33 4D 55 69 71 8E 96 AA B2 CC D4 E8 F0
```

LEYES DE ABSORCION:

El formato sigue siendo el mismo. Los 4 bits de mayor peso indican la

primera operacion, y los 4 bits de menor peso la segunda operacion.

Por la izquierda-izquierda:

   24 2C AC BC BD

Por la izquierda-derecha:

   24 2C AC BC BD

Por la derecha-izquierda:

   44 4C CC DC DD

Por la derecha-derecha:

   42 4A CA DA DB

Por la izquierda-izquierda y por la izquierda-derecha:

   20 28 30 31 32 34 36 37 38 39 3A 3B 3C 3D 3E 3F BE BF

Por la izquierda-izquierda y por la derecha-izquierda:

   13 1B 72 73

Por la izquierda-izquierda y por la derecha-derecha:

   [ninguna]

Por la izquierda-derecha y por la derecha-izquierda:

   [ninguna]

Por la izquierda-derecha y por la derecha-derecha:

   15 1D 74 75

Por la derecha-izquierda y por la derecha-derecha:

   40 48 50 51 52 54 56 57 58 59 5A 5B 5C 5D 5E 5F DE DF

Por la izquierda-izquierda y por la izquierda-derecha y por la
derecha-izquierda:

   33

Por la izquierda-izquierda y por la izquierda-derecha y por la
derecha-derecha:

   35

Por la izquierda-izquierda y por la derecha-izquierda y por la
derecha-derecha:

   53

Por la izquierda-derecha y por la derecha-izquierda y por la
derecha-derecha:

   55

Leyes de absorcion (las cuatro propiedades):

17 1F 60 70 71 9F

NOTAS FINALES:

- No abuses del lenguaje. Si puedes aprende latin, que es mas estricto, y te vale para entablar conversacion con las de letras (aunque, si haces matematicas, no echaras de menos a las de letras).

- Como ya habras notado, en logica de aserciones solo existen dos posibles resultados: verdadero o falso, por lo que el tama¤o del valor total es de 1 bit. Sin embargo, en conjuntos o nivel de bits, el valor total tiene un tama¤o variable (el numero de elementos del conjunto total, o el tama¤o en bits del campo en que trabajemos, respectivamente). No se si ha quedado claro, pero es muy importante entenderlo, porque la igualdad no debe aplicarse a la logica de proposiciones, sino la equivalencia.

- La igualdad ("=") es un operador para formar proposiciones. Compara los dos miembros, siendo la proposicion resultante verdadera si y solo si son iguales. En logica no se utiliza "=", sino la equivalencia:

  "x + 5 = 7" <=> "x = 2"

  Tambien se puede indicar equivalencia logica entre proposiciones mediante el simbolo "ð":

  P ð Q

- En logica se ha trabajado con aserciones. Una asercion es una proposicion siempre cierta o siempre falsa. Una proposicion es un enunciado que puede ser o bien verdadero o bien falso (principio del medio excluido). Existen circunstancias en que la verdad de una proposicion excluye a la otra, por ejemplo: "(x > 3) Y (x < 2)" es una asercion falsa, aunque no podamos decir si cada proposicion por separado es siempre cierta o falsa (por separado no son aserciones, sino solamente proposiciones).

- El significado de "y/o", que suele aparecer en la lista de ingredientes de las cajas de galletas, es el siguiente:

  "aceites y/o grasas" <=> (aceites Y grasas) O BIEN aceites O BIEN grasas

  Al menos es como yo lo entiendo. Esto es la definicion del O inclusivo: "aceites O grasas". Como ves, en el "y/o", el foreslash es un XOR, y ’o’ es tambien XOR.

- En espa¤ol, normalmente interpretamos el ’o’ (inclusivo) como exclusivo, y por esta razon surgio el ’y/o’. Parece que ’y/o’ existe tambien en otros idiomas (en latin creo que no), asi que probablemente sea un error del lenguaje, que en muchos casos la lengua no soluciona.

- El ’o’ exclusivo en logica se suele emplear ’o bien P o bien Q’, aunque en este texto se ha usado ’P o bien Q’. Asegurate de que sean correctos.

- En nivel de bits, la suma modulo 2 bit a bit de dos numeros coincide con la diferencia modulo 2 bit a bit, y se suelen llamar XOR. Probablemente por esta razon, XOR sea conocido como diferencia simetrica o suma exclusiva. Lo de diferencia simetrica debe ser porque todo elemento es simetrizable.

- Lo del numero de operacion me lo he inventado. Es probable que ya existan numeros asignados a cada operacion y que no correspondan a los que he dado yo (en orden de bits inverso). Tambien he llamado a la operacion 15 totalidad, pero ahora pienso que habria quedado mejor completitud.

- XOR y XNOR son muy usadas en criptologia, porque pueden invertirse. Operando el resultado con uno de los operandos se obtiene el otro operando. XNOR es una doble implicacion (equivalencia). XOR es una doble diferencia logica (la diferencia logica y la implicacion son operaciones complementarias, y ambas se pueden dar en los dos sentidos porque no son conmutativas).

- Por que el conjunto vacio esta contenido en todo conjunto? La definicion de inclusion entre conjuntos es: AcB <=> (para todo xîE) (xîA => xîB) Relee la definicion de implicacion si es necesario.

- Creo que me he inventado muchas cosas en las leyes de absorcion. No me gusta la definicion. Si alguien sabe el nombre de cada una, que me lo diga. Tambien no he incluido algunas cosas, como elementos regulares, centrales, y algo mas.

- Le dejo a otro/a lo que queda sobre otros tipos de logica y lo que yo no he escrito sobre logica basica (como cuantificadores). Tambien estaria muy bien aritmetica a nivel de bits.

REFERENCIAS:

[QUE79] Michel Queysanne. Algebra basica. Editorial Vicens-Vives. Segunda edicion. ISBN: 84-316-1789-6. (ha sido una gran ayuda)

[CL] Manuel Castellet e Irene Llerena. Algebra lineal y geometria. Editorial Reverte. Primera edicion. ISBN: 84-291-5009-9.

[BS] Robert G. Bartle y Donald R. Sherbert. Introduccion al analisis matematico de una variable. Editorial Limusa Wiley. Segunda edicion. ISBN: 968-18-5191-9. (tiene un apendice de logica y demostraciones muy bueno)

[BAR96] Pablo Barron Ballesteros. Curso de ensamblador. Segunda edicion. Archivo: CURSOASM.ZIP / CURSOASM.TXT. (el origen de todo esto)

DESPEDIDA:

Probablemente este texto no te servira para mucho, y con conocer and, or, xor, y not te baste, pero he querido ir mas alla. Espero que, al menos, haya servido para modificar tu forma de razonar, y para que veas la logica desde un punto de vista mas real.

Por que aprender el funcionamiento de las cosas creadas por el hombre cuando puedes descubrir por ti mismo la mas pura de todas las ciencias? Se diferente. No te enga¤es diciendote que haces un servicio a la sociedad, que pretendes concienciar al mundo, o que tus objetivos son simples retos intelectuales. Aspira, si puedes, a algo mas.

La criptologia te espera.

Aristoteles "El Filosofo Naturista"

peakaboole@telepolis.com

EOF
madfran

-[0x0A]----------
-[Esteganografia, el poder oculto]----------
-[GRRL]----------SET-26--

ESTEGANOGRAFIA, EL PODER OCULTO

Oppps!!! que bien suena el titulo!, ya me siento realizado... bueno, aqui estamos un articulo mas, para hablar de un tema realmente interesante que en muchos casos no ha tenido la atencion suficiente, pero es un tema que tiene una gran relevancia, mas aun con la llegada de la Info-sociedad.

No!, esteganografia no es una ciencia que estudia la grafia de Estegosaurio, es una ciencia de ocultacion... No!! no son ciencias ocultas, de lo que se trata es de ocultar mensajes, pero no basandose en hacerlos irreconocibles como en la criptografia, sino en hacerlos pasar desapercibidos.

Para entrar en materia, vamos a dar tres definiciones diferentes de la esteganografia desde el punto de vista etimologico, el informatico y el punto de vista cientifico.

Etimologicamente hablando, esteganografia viene de la palabra griega stegos que no significa otra cosa que "cubierta", por lo tanto, el significado de la palabra es "escritura cubierta".

Desde el punto de vista cientifico, esteganografia es el conjunto de metodos y tecnicas para hacer pasar desapercibido o camuflar un mensaje.

Desde luego, informaticamente hablando, no dista mucho de la definicion cientifica, pero desde el punto de vista tecnico, esteganografica electronica consite en incluir un texto en un archivo de tal manera que... bla bla bla

A lo largo de este documento veremos que la esteganografia puede ser mucho mas que las definiciones que se pueden ver en muchos sitios en internet de embedir un fichero en otro.

PRACTICAS DE EMBEDIDO. A.K.A: COMO SE HACE?

Existen miles de maneras de incluir un mensaje, sonido o imagen dentro de un fichero, pero los metodos cabian mucho en funcion del tipo de archivo que nos servira de cubierta. Hoy en dia existen algoritmos para hacer esteganografia en muy diversos formatos de fichero (y mas cosas que veremos). gif, bmp, jpeg mp3, wav, mpeg... y un largo ecetera. Todas ellas utilizan algoritmos mas o menos parecidos, pero en casi todos los casos bastante limitados, no penseis que podeis ocultar una biblia entera en una foto de vuestra familia... de esas cosas hablaremos en el proximo apartado.

Desde luego no es el objeto de este articulo explicar como se incluyen mensajes, ni evaluar los algoritmos, ni testear el software a nuestra disposicion en internet, si no una mera introduccion a este bonito tema.. haw!

Veamos un ejemplo basico de inclusion de un mensaje en un archivo BMP, para ello necesitaremos una foto de nuestra suegra (la mia no, cada uno la suya! y el que no tenga, que utilize otra cosa igualmente amado) y un mensaje. Supongamos que la foto es de 200 x 400 pixels.

Tal y como exige el formato cada pixel es un byte, es decir una ristra de 8 bits algo como (00110101), la imagen se construye con una matriz con todos

estos pixels (recordemos que este formato no contempla compresion de datos).

Con lo cual nos podemos imaginar que una porcion del codigo podria ser algo asi:

```
...
00010101 10100101 01010101 00110101 01110101 01000010 01010011 01101010
00001011 01010101 10100101 01010111 11010111 10000101 01010010 01010010
10101001 10101011 00001001 10100100 00010001 10100101 00010101 10100101
...
```

Cada byte es un color, y donde esta el truco?... todos sabemos que si "retocamos" ligeramente los colores (o sea con colores parecidos), la imagen final no se vera afectada, y tambien sabemos que el bit menos significativo (el que esta mas a la derecha de cada byte) apenas alterara el resultado final de la imagen, o sea que cogeremos de cada byte el LSB (less significant bit), o sea el que esta a la derecha...

No lo dije antes, pero el mensaje que vamos a incluir es "SET", como minimo para incluirlo, necesitaremos tres octetos, uno por cada letra. los caracteres que necesito para repesentarlo en binario son estos tres: 73 65 74
que en binario corresponden con estos tres bytes: 01001001 01000001 01001010

Por lo tanto, retoco mi imagen tal y como hemos contado (retocando el ultimo bit de cada byte):

```
00010100 10100101 01010100 00110100 01110101 01000010 01010010 01101011
       -        -        -        -        -        -        -        -
00001010 01010101 10100100 01010110 11010110 10000100 01010010 01010011
       -        -        -        -        -        -        -        -
10101000 10101011 00001000 10100100 00010001 10100100 00010101 10100100
       -        -        -        -        -        -        -        -
...
```

Como podeis ver los bits que he subrayado, han sido modificados, sin alterarse demasiado el resultado final de la imagen. divertido no?.

Desde luego, este que acabamos de ver es un ejemplo de lo mas basico, la complicacion del algoritmo se puede llevar a limites insospechados, pero ahora vamos a explicar eso que escribi antes sobre que hay muchas maneras diferentes de incluir mensajes:

Sobre este mismo ejemplo, que hubiera pasado si en vez de un mensaje de tres letras necesitara guardar seis?

Facil!, podria haber utilizado los dos bits menos significatvos, esto nos hubiera llevado a tener una imagen con mas distorsion, pero el mensaje valdria igual... Tambien podriamos haber metido el mensaje en la cabeceza del fichero, o despues de la marca de final... O podriamos haber "secuestrado" un byte entero de cada X... esto haria que la imagen tuviera puntos que no tuvieran que ver con la imagen (o si)... eso dependera de el y de la imagen que sea, hay muchas maneras diferentes de incluir archivos, y basicamente el ejemplo que vimos se utiliza en otros muchos formatos de fichero.

Otro ejemplo que podria dar pero que no doy (jesus! que vagancia), es el incluir una marca en un fichero mp3, para luego compartirlo por internet, esto pretende utilizar (o ya utiliza) la SGAE, pero de eso hablaremos mas adelante. El caso es que las marcas son casi imperfectibles y se denotan como "ruido de fondo", si quereis hacer la prueba, lo que teneis que hacer es casi lo mismo que en el ejemplo antes dado.

LIMITACIONES DE LA ESTEGANOGRAFIA A.K.A: HASTA DONDE LLEGA?

Hasta aqui todo ha sido muy bonito, casi podemos guardar lo que nos de la gana en muchos ficheros, nuestras comunicaciones son realmente seguras, y sentimos que aunque alguien husmee en nuestras maquinas no encontrará nada demasiado importante, fuimos felices y comimos perdices... Pues realmente no, realmente, la esteganografia es una tecnica que realmente apenas esta desarollada, estamos en la edad de piedra de la esteganografia.

Realmente, para utilizar de manera efectiva la estaganografia dependes totalmente del tamaño del mensaje, de la imagen, de la paleta de color y lo que yo creo mas importante, el factor humano: De poco vale ocultar algo si luego resalta en su ambiente... Por ejemplo, de nada vale una foto de un paisaje con una calidad altisima en medio de un directorio lleno archivos de otro tipo, el archivo contenedor no debe llamar la atencion.

Como antes he comentado, no es el objeto de este articulo evaluar las aplicaciones de esteganografia. Personalmente, todas las aplicaciones de esteganografia estan severamente limitadas, muchas solo trabajan con unos pocos tipos de archivo o exigen un tipo muy determinado de imagen, aparte que casi todas trabajan exclusivamente con imagnes... y no con otros tipos de archivos. En definitiva, en esteganografia no existe ningun tipo de programa referente y definitivo como puede existir en criptologia -el PGP-, aunque entre todas las aplicaciones cubren un amplio abanico de posibilidades, todas ellas estan bastante sesgadas y se necesita tener un monton de aplicaciones y tiempo para tener un poco de libertad a la hora de incluir mensajes.

Tambien hay que tener en cuenta que muchos algoritmos de esteganografia no "sobreviven" a modificaciones de los archivos de portada que es otro dato muy importante a la hora de escoger un metodo u otro.

Otra limitacion grave de la esteganografia, es sin duda los algoritmos, porque realmente son siempre los mismos, el programa "X" siempre incluye tal dato en la cabecera, y utiliza tantos bytes para "bla bla bla"... y siempre por poco que sea siempre dejan marcas de su paso por una imagen o archivo de portada. esto hace fragil a la esteganografia cuando alquien esta buscando mensajes, por supuesto, la esteganografia es util cuando no te estan buscando... pero eso es otra historia y la cuento mas adelante.

APLICACIONES EN LA VIDA REAL A.K.A: QUIEN Y DONDE SE UTILIZA?

Los que nunca hayais oido hablar de estas tecnicas, a estas alturas estareis pensando que los chicos de SET os estan contando una pelicula, nada mas lejos de la realidad, la esteganografia se utiliza en la vida real y con mejores o peores resultados, Veremos algunos de sus usos reales, como pueden ser las marcas de agua, transmision de mensajes terroristas, deteccion de copyrigths y algun que otro uso.

Marcas de agua

Sabiamente, corporaciones como la RIAA o la SGAE en Espanya rebautizaron la fea palabra de "esteganografia" por "marcas de agua", evitando mancharse al utilizar una palabra muy fea que solo los chicos malos muy malos utilizan.

En la realidad, las marcas de agua y la esteganografia, aunque no son

exactamente iguales (realmente las marcas de agua no son comunicacion, son datos) todos sabemos que en la practica son lo mismo, y las intenciones pueden ser igual de "aviesas" tanto en el usuario de la esteganografia como en las sociedades de autores.

Las sociedades de autores pretenden incluir marcas de agua en todos sus archivos para luego soltar sus "spiders" (programas que buscan patrones) buscando mp3 con sus marcas de agua, cuando las encuentran, se quedan con la direccion de la pagina web para ponerse en contacto con sus administradores y enviarles un mensaje muy poco amistoso sobre abogados, juicios y cosas "mu malas".

Hace poco he leido (creo que en www.barrapunto.com), que la RIAA pretende hacer un nuevo tipo de marca de agua que solo permita la ejecucion del archivo de sonido un numero determinado de veces y despues no funcione. Personalmente creo que este tipo de medidas deberian ir acompanyadas de mas medidas: Prohibir la entrada de alcohol a las reuniones o presentarse a la RIAA en estado de embriagez o sobredosis... ¿una marca de agua que evite la ejecucion de un archivo? ¿cuantos litros de alcohol hacen falta para llegar a esa determinacion?

Reconozco que cosas mas raras se han hecho y hace mucho que ya no voy a clases de informatica (gracias a dios) y que yo recuerde y siempre segun la teoria, un mp3 es la entrada y/o la salida del programa, y como tal, poco tienen que hacer o decidir en la ejecucion del programa. Para esto, hace falta una serie de infraestructuras muy faciles de construir y muy dificil de imponer...

- Necesitariamos un programa que lea el mp3 y que en algun momento de la ejecucion a parte de leer el programa, lea en algun sitio del archivo el numero de ejecuciones que lleva y le sume una ejecucion.

- Cuando llege al numero de ejecuciones maximo, no solo no lo lea sino que destruya el archivo.

Esto romperia por todas partes, calculo que cualquier "avispado" que circula por internet tardaria 5 dias (y estadisticamente me quedo corto, recordemos el DVD) en romper el algoritmo de encriptacion del numero ejecuciones (suponiendo que exista), y ponerlo a 0.

En el supuesto de que nuestro "avispado" no aparezca, rapidamente apareceran players que se pasen por el "forro" contadores o demas historias...

En el peor de los casos, cambiamos el formato mp3 a mp3 encriptado, imagino que para desencriptarlo seria en base al numero de ejecuciones, para que no se evite... para esto necesitarian el un monopolio de players de mp3...
Ese dia, los piratas empezaran a grabar al vuelo, sobre un original en una cadena de musica enchufando la salida al micro del ordenador... pero esto es otro tema, y se deberia hablar aparte, sigamos con otras funciones...

La funcion inicial: mensajes ocultos

Todos sabemos que sobre el atentado terrorista del 11 de septiembre circulan miles de mitos, uno de ellos es el sistema que Bin Laden y sus amigos utilizaron para comunicarse atraves de todo el planeta pasandose por los.... a Echelon, sistemas de deteccion y contraespionaje: Creo que ya sabeis la respuesta: Esteganografia.

Si los rumores que circulan por Internet son ciertos, la manera de utilizar la esteganografia por parte de al quaeda, dista mucho de la de un novato recien sentado delante de un ordenador que solo ha leido el coran en su vida.

No cabe duda que se hizo un uso inteligente de la tecnica, para empezar, no se

limitaronn a incluir mensajes dentro de archivos, si no que los mensajes venian encriptados por si las moscas. Otro gran detalle de su uso muy inteligente, fue el metodo de transmision.

No todo el mundo es administrador de un sitio web, aunque lo tenian realmente facil para eso, solo tenian que crearse una web, que lo puede hacer cualquiera. Eso podria levantar sospechas, por eso necesitaban un sitio con el que no tuvieran nada que ver, pero a la vez pudieran anyadir imagenes al sitio. Por otra parte, su comprensible mania de "trabajar" en lugares muy concurridos da un target muy claro del tipo de web que necesitaban (o necesitan, nunca se sabe) para enviar sus mensjaes: web de venta de segunda mano, sitios como ebay (este es el que citan los rumores), segundamano.com.

Tambien existen rumores que utilizaron sitios porno, estos me parecen menos creibles, dado que para eso necesitarian ser administradores, pero sea lo que sea y cuando el rio suena agua lleva, denota un buen conocimiento de la red de redes, el suficiente para reirse a la cara de las infraestructuras de espionaje que costaron miles de millones.

Deteccion de copyrights

Este caso es muy parecido al primero, las marcas de agua. Muchas empresas de software (y no voy a citar nombres... bueno, si, por ejemplo Microsoft) incluyen la licencia del producto, e incluso en algunos caso datos personales de la persona que creo el archivo.

Las utilidades de esto son muy amplias y parecidas a las del primer caso, no voy a decir nada sobre incluir el numero de licencia en un archivo, entiendo que la industria puede y debe defenderse... pero lo que ya no me parece de recibo es la absoluta violacion de la intimidad guardando datos extras que el usuario inocente cede con toda su buena voluntad mas aun cuando estos estan ocultos y solo un cierto tipo de personas pueden leerlo. Una cosa es que cuando utilizas un programa shareware te ponga una etiqueta en la pantalla, o un aviso y otra es que publique tus datos.

Existen otras utilidades, pero en todo caso menores y que no citaremos en este articulo.

ESTEGANOGRAFIA MANUAL

Ya he comentado antes, que no creo demasiado en las aplicaciones de esteganografia, por si tienes la mente olvidadiza, la razon es que estas son bastante limitadas.

Sin embargo, si creo en otro tipo de esteganografia, por llamarla de alguna manera la esteganografia "manual", la esteganografia hecha a mano, existen muchos sistemas para ocultar informacion, y no tiene porque ser en los archivos tipicos de sonido imagen o video, puedes esconder mensajes, claves o lo que quieras en otros documentos como .exe, .xls, txt y un largo etc, solo necesitas conocer a conciencia el formato del archivo. para hacer un uso efectivo de estas tecnicas lo que necesitas es ser creativo, y hacerlo en los sitios mas insospechados de todos. por ejemplo Tengo un amigo que le da por guardar claves en la zona de "X" del archivo msdos.sys con todo su morro y sin encriptar, a mi la verdad, me parece efectivo.

No creo que haga falta grandes seudocodigos para encriptar, porque realmente su valor no esta en su calidad de ocultacion, si no en la capacidad del "cazador" para encontar. Un codigo de ocultacion deja de ser efectivo cuando es conocido, y esta es de las pocas excepciones a la seguridad basada en la

ocultacion, o al menos esta es mi opinion, se que torres mas altas han caido... pero a modo chapuza, es mas que efectivo, a menos claro, que te esten buscando las cosquillas a conciencia.

Tampoco creo que haga falta ser un genio para lograr incluir un archivo dentro de otro, durante algun tiempo, he utilizado una imagen de photoshop para guardar "cosillas", al fondo de todas las capas, puse una transparente, con unos textos que deseaba salvaguardar de los demas.

Otra forma, un tanto estupida, todo hay que decirlo, es interpretando palabras, veamos un ejemplo.

"yo te quiero, tu me odias, tu me quieres, yo te odio. Realmente tu no entiendes lo que yo siento, y creo que yo me siento dolido por lo que tu sientes, el dolor que tu sientes a mi me parece una mierda al lado del que yo siento".

Veamos, hasta aqui vemos algo parecido a una carta de amor un tanto boba, nada anormal. Ahora, vamos a sacar de este texto los "yo" y los "tu", Algo asi:

yo tu tu yo tu yo yo tu tu yo

Y si ahora interpretamos los yo como un 1 y los tu como un 0 nos quedaria:

1 0 0 1 0 1 1 0 0 1

De esto a un mensaje cifrado ya hay poco. Desde luego tal y como esta redactada la carta, el cazador solo puede pensar dos cosas una es que su victima es idiota, y la otra es que algo huele mal, para hacerlo mas disimulado (vuelvo a repetir que la creatividad es lo que importa), el texto deberia ser mucho mas largo y que su redaccion pueda ser lo suficientemente implicita en el contexto, como para no llamar la atencion.

Saliendonos del tema informatico, y por si alguno cree que esto es algo muy moderno, nada mas lejos de la realidad, la esteganografia, ya era utilizada por los Griegos, se utilizo durante la edad media, e incluso los Alemanes utilizaron intensivamente tinta invisibe durante la segunda guerra mundial ...

BUENAS PRATICAS EN EL USO DE LA ESTEGANOGRAFIA.

Si alguno ha decidido que a partir de ahora va a hacer pasar "despercibido" alguno de sus ficheros, estos pueden ser algunos buenos consejos a tener en cuenta:

- Evita que tu archivo de cubierta resalte en el contexto, es decir, no pongas tu imagen en un directorio de documentos, porque aunque para ti lo sea, para otros no. Este consejo que parece tan obvio, no lo es tanto.

- La esteganografia electronica es mucho mejor para ocultar cosas a la vista de otros que como metodo de transmision, ademas corres el riesgo que te confundan con una celula de al caeda :-)

- Hazte tu propio sistema, evita programas demasiado conocidos. Realmente no sabes a que nivel esta el que busca mensajes, no sabes si los que controlan Echelon tienen mil herramientas funcionando, la manera efectiva es no utilizar nada conocido, nadie conoce el software utilizado por redes de espionaje.

- Si trasmites estaganografia, nunca esta de mas que de paso encriptes tu

mensaje.

- Recuerda, que en el caso de no ser legal (dudo que en muchos paises exista ningun tipo de legislacion sobre esto) siempre se puede apelar a la casualidad y al desconocimiento. :-)

ALGUNOS LINKS

Para los que os apetezca seguir tirando del hilo sobre este tema, aqui teneis unos cuantos links sobre el tema, aunque ya os advierto que la informacion que circula esta muy difusa y casi toda en ingles.

http://www.jjtc.com/Steganography/ --> Un sitio bastante bueno.

http://www.StegoArchive.com --> Bastante completa.

http://steganography.com/ --> Para ir de compras.

http://www.privacyexposed.com/resources/steganog.htm --> Muchos links.

Tambien podeis probar las muchas respuestas que da google sobre este tema.

GRRL
web@set-ezine.org

EOF

-[0x0A]----------
-[[Paseando por la red]]----------
-[madfran]----------SET-26-

INTRODUCCION

No siempre se encuentra lo que se desea ni se destapa lo que se quiere. La mayoria de las veces cuando navegamos por estas redes tenebrosas, lo unico que encontramos es una coleccion de dibujos, fotografias y montajes, que solo disparan una cantidad enorme de colores y movimientos sin mas objeto que reclamar nuestra atencion pero sin ninguna intencion de darnos nada a cambio. Normalmente el aburrimiento nos puede y mecanicamente nos encontramos introduciendo en los campos que nos presentan las web, codigos que no tienen ninguna similitud con nuestro nombre y apellidos.

Un observador casual se preguntara para que introducimos esta serie de caracteres extravagantes en el sitio donde una pringosa web esta intentando enterarse de nuestros datos mas intimos. Que pretendemos con esta serie de %20 /, ? y demas cosas que no dicen nada a los comunes mortales, es bastante evidente. Estamos intentando explotar alguno de los miles de defectos que adornan las web de esta tierra (otras no conozco) para enterarnos de algunas tonterias, como la password del administrador, la cuenta bancaria de algunos cientos de confiados usuarios o el numero de la tarjeta VISA de unos miles de incautos que han comprado alguna tonteria en esta o aquella infame web.

TECNOLOGIA WEB

A pesar del tiempo que lleva en marcha la red de redes, los protocolos sobre los que se basa la web son todavia de forma fundamental los viejos y queridos HTTP que trabajan a traves del puerto 80 y su hermano gemelo HTTPS que se comunica a traves del puerto 443. Ya pueden introducir los firewalls que les de la gana y las protecciones que deseeen, pero siempre deben dejar estas dos puertas para poderse comunicar con el exterior y siempre que alguien deja una puerta abierta,... un indeseable pueda aprovechar el momento.

Si hacemos un poco de historia y recorrido de protocolos, nos encontramos que existen diversas versiones del mismo protocolo. Para el HTTP, tenemos :

HTTP/0.9
Nunca he sabido el porque de este numero de version tan heterodoxo, pero el caso es que fue el primero en salir ahi por el anyo 1990. Sus especificaciones se encuentran en el documento RFC1945 que si teneis ganas de leer, podeis encontrar en,
www.ietf.org/rfc/rfc1945.txt
Hasta 1996 su uso fue mas bien modesto debido al estado infantil en que se encontraba por aquel entonces la red. Eran tiempos en que todo se hacia a base de telnet y de menus con nulos contenidos graficos

HTTP/1.0
Se presento en sociedad en Mayo de 1994 y a pesar de su avanzada edad (en terminos informaticos), sigue siendo el rey de los protocolos HTTP en la red. Esta va a ser el arma de aprendizaje para controlar el funcionamiento del sistema cliente/servidor. En el mismo documento antes mencionado (rfc1945), podreis encontrar las especificaciones.

HTTP/1.1
Oficialmente salio en 2001 (no se en que mes) y es la ultima version de este protocolo. Esta documentada en el RFC2616, que podeis encontrar en la misma web antes aludida. Existe una diferencia fundamental con respecta a las versiones anteriores y es que soporta el paso de parametros con el query '?'. Este hecho es el motor de muchas de las

aplicaciones que se encuentran en la red y es el principal punto de apoyo para iniciar ataques en toda regla.

Para el HTTPS solo existe una version, que se encuentra especificada en el documento RFC2246. En el fondo este protocolo es un trafico HTTP cifrado. Con lo cual solo emisor y receptor son capaces de entenderse y no existe la posibilidad de que terceros a la escucha se enteren de nuestro trafico. Los mensajes se cifran mediante una especificacion SSL (Secure Sockets Layer) de la cual hay diversas versiones con sus protocolos (SSLv1, SSLv2, SSLv3)

Si nos centramos en los protocolos HTTP sin cifrar, lo primero de todo es comprobar que version esta corriendo en la maquina que deseamos visitar. Todo el mundo debiera saber que lo que vemos en nuestro navegador no es lo que realmente recibe nuestra maquina sino una interpretacion de lo que le llega. En el fondo es como las personas, no decimos lo que vemos o hemos visto, sino que damos nuestra interpretacion particular, de forma gratuita. Dejando a parte las digresiones que tanto me gustan pero que a ninguna parte llevan, lo que nos hace falta es un interprete que no ponga nada de su parte, eso existe (al menos en el mundo de la informatica de redes) y se llama netcat. Es una herramienta que podeis encontrar en el disco duro de mi PC, pero como no tengo intencion de daros acceso al mismo, lo mejor es que lo busqueis en algun sitio de confianza tipo www.l0pht.com o algo por el estilo, en todo caso podeis buscar en google pero tened cuidado con lo que os bajais porque hay versiones con troyanos incluidos gratis en el paquete.

Una vez teneis el netcat en vuestras manos solo teneis que teclear,

```
nc.exe www.ejemplo.com 80
GET / HTTP/1.0
y darlo dos veces al return
```

Como respuesta el servidor os devolvera una informacion parecida a esta,

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: http://191.11.12.2/
default.htm

.... y otras informaciones
```

Con todo esto ya podeis saber conque tipo de maquina os enfrentais (tambien han podido falsear los header, pero esto es otra historia) y podeis empezar a planificar el ataque. De momento es bueno saber que tipo de comandos podeis emplear.

Si os enfrentais a servidor HTTP/1.0 podeis utilizar,

GET Devuelve el contenido del archivo solicitado. Si se pide un archivo html devolvera el contenido pero si es un archivo ASP, el servidor procesara el archivo y enviara el resultado de la ejecucion del archivo Atentos a la diferencia !

HEAD En este caso no devuelve el contenido del archivo sino el resultado de informacion generica del servidor. COn esta informacion se puede empezar a trabajar !

POST Solicita al servidor aceptar una cierta informacion para realizar algunas tareas con ella. Normalmente se utiliza en contexto de scripts CGI.

Si estais frente a un HTTP/1.1 , hay mas opciones,

CONNECT Utilizado si queremos jugar con un proxy que tiene las suficientes habilidades para hacer switch dinamico.

DELETE Sirve para borrar cosas, pero casi nunca esta activada en los servidores modernos, por motivos obvios.

GET Mismas funciones que en el caso del protocolo HTTP/1.0.

HEAD Mismas funciones que en el caso del protocolo HTTP/1.0.

OPTIONS Informa de las opciones disponibles. Si ponemos un *, nos informara de todo lo que esta implementado en el servidor. Por tanto es sumamente practico como punto de partida.

POST Mismas funciones que en el caso del protocolo HTTP/1.0.

PUT Crea un fichero con el contenido (casi) que le solicitemos. Para registrar salidas que luego van a ser entradas de otras scripts es bastante practico.

TRACE Envia una peticion de mensaje loopback. Es muy util para descubrir los proxys en linea.

ALGO SOBRE CARACTERES ESPECIALES

Despues de conocer que tipo de adversario tenemos, es bueno conocer que tipo de informacion podemos utilizar. Cualquier tipo de archivo html no es otra cosa que un conjunto de caracteres alfanumericos, pero como de costumbre e incluso entre los seres humanos ocurre, no todos los caracteres son iguales ni tienen la misma importancia ni siquiera un comportamiento parecido.

En el caso de la tecnologia HTTP es bueno repasar algunos caracteres,

? Es un separador query. Todo lo que se encuentra a su derecha se interpreta como una peticion query a una base de datos o de entrada a un programa.

& Separador de parametros. Muy util si queremos enviar varios parametros al mismo tiempo y no deseamos que se mezclen de una forma obscena e inutil para nuestros propositos.

= Separa el nombre de un parametro de su contenido y de paso lo asigna para que posteriormente pueda ser tratado de forma decente.

+ Se transforma en un espacio (casi siempre).

: Separador de protocolo. Ya sabeis, lo que esta antes normalmente es un http, pero a veces es un https e incluso ftp.

Se utiliza para indicar un punto concreto de arranque dentro de un mismo archivo. O sea .....index.html#1 es distinto de ...index.html#2 pero se encuentra dentro del mismo archivo index.html

% Es un caracter de escape para indicar que a continucion se encontrara una notacion hexadecimal.

@ Bastante famoso, no? Se utiliza para direccion de correo electronico

~ En ambientes tipo unix, indica un directorio personal

Tambien es bueno saber algo de los metacaracteres,

* Es un caracter comodin

; Su significado difere en funcion de la aplicacion. Para lenguajes como C o perl es un indicador de final de linea. En scripts Bourne o queries SQL es un separador de comandos.

| Es un caracter pipe para encadenar el resultado de un comando con la entrada de otro.

’ El caracter acento grave se utiliza como comando de substitucion de salida. Poniendo un ejemplo clarificador si conseguimos que el servidor trague con un comando tal como

```
files=’ls -la’
```

conseguira que el resultado de la instruccion ls -la pase a engrosar el contenido del fichero files.

Todo programe que corra en un servidor que se precie de serlo, debe controlar que no se le envien este tipo de caracteres, pero esto no es el caso de muchisimas aplicaciones que todavia se encuentran activas. Si encontramos alguno de estos servidores con exceso de espiritu de colaboracion y capaz de prestar todo tipo de informacion, solo hace falta saber un poco sobre el sistema operativo a atacar y en poco tiempo se tendra completo acceso.

Sin embargo estos son tiempos pasados y salvo los servidores carentes de cualquier interes, los mas serios han aprendido la leccion y cuidan sus scripts, sin embargo al poco tiempo aparecio otro tipo de problema. Los caracteres Unicode.

CODIFICACION UNICODE

La codificacion ASCII hexadecimal es mas que suficiente para dar servicio al alfabetico latino (con todas sus variantes) a la numeracion arabiga y a algunos caracteres mas de uso normal, como los operadores matematicos. El problema empezo cuando se quiso dar servicio a todo tipo de alfabetos y caracteres esotericos para lo cual hubo que hechar mano de la codificacion UTF-8 (Universal Character Set Translation Format). A pesar que UCS esta mantenido por ISO, hubo un grupo de empresas (fundamentalmente vendedores de software) que se dedicaron a estudiar la posibilidad de unificar la representacion de una serie de codigos bajo un unico esquema. Este grupo se conoce como el Unicode Consortium (www.unicode.org).

Sin entrar en como funciona este galimatias, lo importante es darse cuenta (como se dieron cuanta algunos) que el mismo caracter se puede representar en un unico byte, con dos o con tres. Fue asi como un avispado, hacia el Octubre de 2000, descubrio que el caracter ’/’ se representa como el 00101111 en binario, como 47 en decimal y 2F en hexadecimal.

Todo esto en un unico byte, pero queria decir lo mismo 1100000 10101111, o 49327 o C0 AF si se emplean dos bytes. Reflexionando sobre el tema se le ocurrio poner en el navegador %C0%AF y el servidor que solo controlaba el paso de un escualido 2F, dejo pasar el ’/’ y el tipo en cuestion consiguio entrar en muchos sitios que antes le estaban vedados y seguidores suyos crearon el gusano Code Red. Este es la famosa vulnerabilidad Unicode.

Un ejemplo muy sencillo de la explotacion de la vulnerabilidad es,

```
http://www.servidor.com/scripts/..%C0%AF../winnt/system32/cmd.exe?/c+dir+d:\
```

Esta sencilla conbinacion, nos lista el contenido del directorio raiz del disco d: de un servidor con windows NT con su software sin actualizar (ya hay pocos de esos, tampoco os molesteis conmogo si no encontrais ninguno a las primeras de cambio).

ALGO MAS QUE APRENDER

Los programadores que tienen que crear los pesados conjuntos de caracteres que configuran los modernos programas, se valen normalmente de tecnologias bastante standard. Siempre es bueno saber de estamos hablando antes de empezar a teclear codigos a diestro y siniestro. He ahi una forma basica de reconocer la tecnologia empleada.

Si vemos que en la URL del navegador hay algo que termina con una cierta extension, podemos deducir lo que tenemos al otro lado de los cables.

Extension	Technologia	Plataforma
.pl	Perl CGI script	Generico. Normalmente UNIX
.asp	Active Server Pages	Microsoft IIS
.aspx	ASP+	Microsoft .NET
.php	PHP script	Generico. Normalmente Apache
.cfm	CodFusion	Generico. Normalmente Microsoft IIS
.nsf	Lotus Domino	Servidor Lotus Domino

CASO PRACTICO

Supongamos una URL de aquellas cutres de hace anyos que tiene un aspecto tal como, www.servidor.com/cgi-bin/login.cgi

La pantalla de nuestro navegador muestra la tipica ventana donde se pide el nombre de usuario y el password invitando a validar todo mediante un boton standard login. Supongamos que introducimos como usuario ’pepe’ y como password ’nena’. Si, a continuacion, en lugar de dar al login le damos en el menu a Ver/Fuente (suponiendo que nuestra configuracion sea en castellano) veremos el listado del fichero html y cuyo aspecto puede parecerse a este.

```
<form method=POST actions="/cgi-bin/login.cgi">
<table border=0>
<tr>
<td>Nombre:</td> <td>input name=user type=text width=20></td>
</tr>
<tr>
<td>Password:</td> <td>input name=pass type=password width=20></td>
</tr>
</table>
<input type=submit value="login">
</form>
```

O sea estamos intentando pasar las variables ’user’ y ’password’ y cada una de ellas tendra el valor de ’pepe’ y ’nena’. La primera variable es de tipo text y la segunda de tipo password, aunque la unica diferencia es que el contenido de la primera variable se ve en la pantalla y la segunda no, impidiendo que cualquier fisgon mire por encima de tu hombro. Por lo demas no ofrece ningun tipo de proteccion adicional.

Lo importante de esta historia es que se puede enviar la informacion a traves de la ventana del navegador o bien mediante la siguiente URL

http://www.dominio.com/cgi-bin/login.cgi?user=pepe&password=nena

Poder lanzar peticiones de login sin tener que pasar por la pantallita es el punto de partido para poder planificar ataques de fuerza bruta en linea.

RECUENTO FINAL

No vamos a explicar con detalle todo lo que se puede hacer, se ha hecho, se esta haciendo y se hara en el futuro. Como en casi todos mis articulos, lo unico que pretendo (con escualidos resultados) es despertar la curiosidad de alguien para que continue el camino que yo solo he senyalado.

Solo hace falta quedarse con unos pocos conceptos.

- Lo que veis en el navegador solo es la interpretacion de un codigo.
- Este codigo puede ser by-pasado mediante caracteres insertados directamente en la URL del navegador.
- Los codigos pueden construirse con distintos esquemas, pero los programadores preferentemente utilizan tan solo unos pocos por aquello de 'que inventen ellos'.

Para que no os quedeis con mal sabor de boca, os dare algunas direcciones utiles que os pueden servir tanto para profundizar un tema concreto como para descargar herramientas automaticas.

UTILIDADES

www.foundstone.com
	SuperScan	Un scaner de puertos TCP muy popular bajo Windows
	FScan	Un scaner en linea de comando. Tambien bajo Windows

www.wiretrip.net/rfp/
	Whister	Un scaner para vulnerabilidades de web. Escrito en PERL

www.nstalker.com/stealth/
	Stealth Scanner	Scanner de vulnerabilidades de web.

www.nessus.org
	Nessus Scanner	Scanner de vulnerabilidades.

www.cerberus-infosec.co.uk
	Cerberus	Scanner de vulnerabilidades de web y de bases de datos.

www.nextgenss.com
	Typhon I	Similar a Cerberus

www.insecure.org/nmap/
	Nmap	Creo que es el mejor scanner que incluye todo tipo de servicios e identificacion de sistemas operativos

LINK Y RECURSOS

http://www.packetstormsecurity.org
http://www.securityfocus.com
http://www.securiteam.com
http://neworder.box.sk
http://www.cert.org
http://www.wiretrip.net/rfp/

HERRAMIENTAS AUTOMATICAS

Netcat	Herramienta para efectuar conexiones sin ningun tipo de interface. Es

muy util para automatizar ataques o para ver codigos ocultos.

Whisker Es un buscador de vulnerabilidades que corre bajo Unix y Windows. Puede utilizarse para realizar ataques de fuerza bruta.

Brutus La ultima vez que lo busque lo encontre en www.hoobie.net/brutus
Es uno de los automatas de ataque mas completos

Achilles
Actua como un proxy, de forma que permite modificar la informacion que recibe antes de devolver la respuesta. Las posibilidades posibilidades son las siguientes :
- Servidor proxy (puerto configurable)
- Interceptacion de trafico HTTP y SSL
- Insercion y modificacion de datos en linea
- Recalculo de campos HTTP
- Chequeo de buffer overflow
- Registro de sesiones HTTP y SSL

Cookie Pal
Se utiliza para controlar los cambios que se producen en los cookies que recibimos.

Teleport Pro
Muestra todas las referencias que existen bajo una direccion URL

EOF

-[0x0C]----------
-[Ataque a SET]----------
-[madfran]----------SET-26--

HUBO UN TIEMPO EN QUE TENIAMOS ENEMIGOS,.....

INTRODUCCION

Si senyores. Hubo un tiempo en que eramos alguien y hasta teniamos enemigos. Hoy parece que solo llamamos la atencion de pesados que se dedican a mandar mensajes idiotas a nuestro tablon de anuncios. La vida es como es y no como quisieramos que fuera. De todas formas vale la pena rememorar los aciagos acontecimientos que acaecieron hace mas de un anyo (como pasa el tiempo!) y que contribuyeron a hacernos perder el tiempo, las energias y un poco de salud.
Como todo el mundo sabe (espero) estamos hablando del secuestro de nuestro legitimo dominio por parte de un personaje que tuvo la idea de descargar el mal humor acumulado por largas noches de IRC, contra todo un equipo de gente que ni conocia su existencia ni tenia nada que ver con el asunto.

UN DESPACHO CUALQUIERA

Si. En un despacho cualquiera, de una empresa como existen tantas. Era un caluroso dia de primavera, las epocas de agobio por una sobrecarga de trabajo se encontraban en el pasado y habia un poco de tiempo antes de que a la empresa se le ocurriera algun nuevo encargo en algun lugar de este planeta. En resumen, habia tiempo para zanganear un poco y rastrear internet en busca de alguna novedad. Este tipo de actividad, no se sabe como, pero acaba generando una enorme cantidad de trafico mensajero debido a la serie de web empenyadas en buscar nuestro perfil a cambio de dejar ver lo que se esconde tras sus ofertas (normalmente, poca cosa). Aburrido de borrar y configurar el cliente de correo para que borrase automaticamente por mi, me encuentro de repente de un mensaje de gnd.

Primero una lectura apresurada,... despues un poco de calma y me entero realmente de que va la historia. Pues si, parece que nuestro dominio, merece la misma consideracion que la merecio en su dia la web de la Guardia Civil en Espanya y si se apunta el navegador hacia www.set-ezine.org, aparece algo que no es lo que uno se espera (al menos yo, ... pobre infeliz).

Como no era la primera vez y teniamos alguna experiencia en este tipo de problemas, la historia, mas que cabrearme, me sorprendio un poco, ya que no acababa de entender la porfia de algunos personajes en dar la vara a diestro y siniestro. Pero en fin, cada un es como ha nacido y como las circunstacias de la vida lo han moldeado y hay algunos moldes que no consiguen generar mas que odios y rencores.

PREGUNTAS Y RESPUESTAS

El contenido de la falsa web de SET no era nada del otro mundo. Una falsa presentacion firmada por un tal OTT (suena a empresa de trabajo temporal) alardeando, con un monton de faltas ortograficas, que pertenecio en algun momento al antiguo staff de SET. Nunca hemos sido muy ordenados en SET, pero cuando falta alguien nos damos cuenta y no habiamos encontrado a faltar a ninguno en los ultimos meses, pero en fin! si OTT dice que pertenecio al grupo de gente que regularmente contribuyo con algun articulo a SET, pues habra que dar fe y confianza en su palabra.

A continuacion una serie de logs manipulados y una serie de mensajes que en

teoria deberia haber recibido y no constan en mi historico, lo que me indica, eso y la falta total de cifrado y de firmas, que probablemente eran mas falsos que las monedas de 3 euros. Tampoco es cuestion de ensanyarse demasiado, si alguno tiene interes, todavia guardo copia de del contenido, y puedo enviarle copia de todo el desmadre.

Como se habia llegado a esta situacion ?,... sencillo. En aquella epoca el dominio de SET estaba registrado en NetworkSolutions. Si alguien hacia un whois utilizando, por ejemplo el servidor whois.networksolutions.com, buscando el dominio de set-ezine.org, se encontraba con una informacion tal que

```
domain:               set-ezine.org
owner-address:        xxxxxxxxx
owner-address:        xxxxxxxxxx
owner-address:        xxxxx
owner-address:        xxxxxxxx
owner-address:        xxxx
admin-c:      xxxxx
tech-c:               xxxxx
bill-c:               xxxxx
nserver:      EU1.M2KCORE.COM 216.167.104.120
nserver:      SP1.M2KCORE.COM 216.167.76.148
reg_created:  2001-07-10 07:50:02
expires:      2002-07-10 07:50:02
created:      2001-07-10 13:50:03
changed:      2001-07-10 13:50:03

person:               Juan Enrique Gomez
nic-hdl:      xxxxxxx
address:      Metropoli2000 Networks, SL
address:      Capitan Haya, 58 - 6F
address:      28020
address:      Madrid
address:      Spain
phone:                +34 914250023
fax:          +34 914250136
e-mail:               juanen@metropoli2000.net
```

Que significaba todo esto ? Pues que teniamos un nombre de dominio, una direccion IP, pero como eramos (y seguimos siendo) pobres de solemnidad, no disponiamos de maquina alguna donde tener nuestro web colgada y por tanto alquilabamos un trocito de espacio virtual en otra maquina (a bajo costo, que dicen los entendidos) desde donde salian los bits cuando alguien clicqueaba sobre le direccion www.set-ezine.org
Dicha maquina virtual pertenecia a metropoli2000 y era ahi desde se manejaba todo el cotarro y por ello aparecia la direccion de contacto tecnico que debia encargarse de los aspectos liosos de redireccionamiento y demas.

Todo sencillo, limpio y explendoroso. Lo malo es que si se intentaba hacer la misma operacion unos dias mas tarde lo que aparecia era algo diametralmente distinto.

```
Domain Name: SET-EZINE.ORG
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: DNS1.ENOM.COM
Name Server: DNS2.ENOM.COM
Name Server: DNS3.ENOM.COM
Name Server: DNS4.ENOM.COM
Updated Date: 14-aug-2001
```

Veis la diferencia? Habian desaparecido las referencias especificas de nombre de contacto? motivo? Pues que el dominio ya no estba registrado en NetworkSolutions sino en ENOM.

El mecanismo para hacer este cambio espectacular es de lo mas banal y no dice nada bueno sobre la seguridad del registro de los dominios. En teoria para cambiar los datos hace falta un documento firmado, pero en la practica basta con un fax garabateado. Y esto es precisamente fue lo que sucedio. Alguien con mucho tiempo libre, tomo papel y boligrafo, garabateo una orden a NetworkSolutions indicandole dos cosas,

- El cambio de host donde apuntar www.set-ezine.org
- Simultaneamente solicitaban que se cambiara de organizacion de registro y se transfiriera a ENOM

NetworkSolutions, envio un mensaje a gnd, pidiendole confirmacion del cambio, pero entre las supuestas virtudes de nuestro antiguo editor, no estaba ni esta la del orden y concierto. Los mensajes en su buzon se acumulaban sin que se molestara en leerlos y pasado un cierto tiempo y a pesar de que el mensaje no habia rebotado sino simplemente no habia sido contestado, NetworkSolutions sin realizar nuevos intentos de ponerse en contacto con el administrador de de nuestro dominio en metropoli2000, realizo todos los cambios.

Hasta aqui, digamos que estabamos empatados. Gnd por su desidia en la lectura del correo y Network por su falta de interes en pedir confirmaciones de ningun tipo acerca del cambio, aunque este resultaba de lo mas sospechoso.

MANOS A LA OBRA

El resultado fue de lo mas molesto ya que por un lado NetworkSolutions se lavaba las manos como Pilatos, cuando le pediamos que comunicara a ENOM el atropello cometido (no querian reconocer el error) y por otro ENOM solo sabia que alguien le habia transferido el registro del dominio y le habia indicado hacia donde apuntar. Dado el contenido de la web, era mas que evidente quien tenia razon y ademas todos los datos del nuevo propietario eran falsos y nadie contestaba a los posibles esfuerzos de contacto por parte de ENOM, pero ahi tropezamos con la burocracia de ENOM y un problema de idiomas. Nadie en ENOM se interesaba en una web escrita en castellano.

Como podreis ver no era un simple problema de decir, escribir, comentar, gritar certificar, ... quienes eramos y quien era el verdadero duenyo del dominio. ENOM no poseia ningun documento que certificara quien era el propietario y tampoco realizaba muchos esfuerzos para comprobar la verdad. Simplemente dejaba pasar el tiempo para comprobar quien se cansaba antes. Un viejo truco consiste en esperar a que el registro caducara por falta de pago y a partir de ahi el primero que da la cara y pone el dinero encima de la mesa, se lleva el dominio y la pelea se termina.

Nosotros no estabamos dispuestos a llevar a estos extremos, mas que nada porque habia que esperar todo un largo anyo, empezamos de entrada a dar la paliza a los que alojaban a la web. En este caso se trataba de los chicos de http://www.freewebz.com, como buenos comerciales que pretenden ganarse la vida con la publicidad, si se dieron cuenta que la historia olia mal y despues de algunos mensajes y de un par de fax de protesta, eliminaron los contenidos de la web.

Sin embargo nuestro comun amigo no se dio por vencido (desde luego tiene unas ganas de fastidiar y una perseverancia que merecen mejores empresas) y redirecciono la web www.set_ezine.org hacia http://defaced.alldas.de/mirror/2001/07/31/www.armornet.tm.fr/

Tambien es verdad que si el objetivo era bastante molesto para nosotros, la idea estaba bien concebida y razonablemente bien ejecutada.

Aqui la gente de DEFACED trabajaron con una falta de profesionalidad increible y simplemente se negaron a revisar sus log y sus bases de datos a pesar de que era evidente de que alguien habia manipulado todo el conjunto de datos (no cuadraban las fechas de anuncios y habia todo un lio entre el 31 de Julio y el 20 de Agosto). Yo creo que ni siquiera entendian medianamente bien el ingles y mucho menos el mecanismo que se habia seguido para realizar el desaguisado.

RESOLUCION

Finalmente no se si por perseverancia, porque era evidente que teniamos mas razon que un santo o por un cumulo de casualidades, ENOM devolvio el control a NetworkSolution y este redirecciono todo hacia metropoli2000.

Todo ello ocurrio el 23 de Octubre de 2001. Casi cinco meses mas tarde.

En todo eso a nosotros nos quedo una duda. Desde donde salio el fax que inicio el desaguisado?. Todo el mundo sabe que esta informacion queda registrada en el texto impresa del punto de destino, por lo tanto no habia mas que pedir a nuestros amigos de NetworkSoltuions el envio de una copia del orginal. Parece que tenian la conciencia sucia, ya que no nos costo mucho obtener la informacion. El numero fatidico es el 934184435 y corresponde a la Asociacion de Fotografos Profesionales de ESPANA. No creemos aue esta benemerita asociacion se dedique a robar dominios ajenos, pero probablemente hay ahi alguien que en algun momento tuvo acceso a su fax. Si alguno de vosotros sabe mas del asunto, pues no tiene mas que decirlo.

ALGUNOS COMENTARIOS FINALES SOBRE EL ICAN

El lio de la gestion del sistema de registro de nombres de dominio tiene su origen en la forma en que han nacido los organismos encargados de la organizacion de los nombre en internet. Inicialmente la NSF (National Science Foundation) de los Estados Unidos quien estuvo al cargo de las bases de datos donde se encuentran los parametros de los dominios de primer nivel (se llaman de primer nivel a los sufijos .com .net .org y alguno mas que ahora no viene al caso). La tarea parece que sobrepasaba la capacidad del director del sistema, Jon Postel (o tal vez se canso de trabajar por amor al arte, como en SET) y lanzo una propuesta. La creacion de tres organismos que pusieran en marcha una organizacion independiente y sin animo de lucro que fuera capaz de realizar la tarea que el hacia en sus ratos libres. Su propuesta formal fue :

- Internet Society
- Internet Architecture Board
- Internet Engineering Task Force

Yo diria que Postel no calibro bien la tarea. No tanto la tarea fisica como el galimatias de organizacion, discusiones esteriles, reuniones inutiles. Solo una muestra de lio que se ha organizado (y que ni yo mismo entiendo) es que se creo el International Ad Hoc Committe formado por la Internet Society, la Organizacion Mundial de la Propiedad Intelectual y la Union Internacional de Telecomunicaciones. El motivo fue crear a su vez una ONG, bajo ley suiza en 1997.

Postel tuvo que realizar un trabajo a dos bandas, por un lado, discutiendo con NetworkSolutions que dirigia por aquel entonces la base de datos de los dominios .com, la IANA y el Boston Working Group. Networksoltions estaba

dirigida por antiguos directores de los servicios secretos y militares de EEUU o sea no eran ningunos nenes de teta y sabian discutir y presionar. Se llego a un grado tal de falta de entendimiento que en febrero de 1998, Jon Postel pidio a los administradores del sistema que no apuntasen los servidores de dominios de raiz a las maquinas de NetworkSolutions sino al servidor de la Internet Assigned Numbers Authority. La situacion se mantuvo mas de una semana, pero Postel consiguio demostrar que le red funcionanba igual de bien (o de mal).

Finalmente se formo la ICANN (Internet Corporation for Assigned Names and Numbers). Postel queria una organizacion cerrada, una oligarquia de ingenieros. Finalmente, en noviembre de 1998, el Departamento de Comercio reconocia a ICANN e iniciaba la independencia del Sistema de Nombres de Dominio. En el acuerdo con el gobierno se especifica que la mitad de sus 18 directores saldrian de elecciones publicas. Nada mas empezar, la corporacion reducio el numero a 5.

Las hipoteticas elecciones se celebraron el 2000, pero no fueron un modelo de orden y concierto. La votacion se celebro por internet, intentando demostrar la viabilidad de dicha tecnica, sin embargo lo unico que demostro fue las dificultades tecnicas que acompanan a las votaciones sin soporte fisico. Casi doscientas mil personas se inscribieron pero tan solo algo mas de treintaicuatro mil superaron el complejo procedimiento.

Cuatro anyos mas tarde, esto parece un horno de grillos. Luchas internas, zancadillas, traiciones, mueven al presidente Stuart Lynn a llamar a la reestructuracion, ofreciendo un tercio del consejo a los gobiernos y aboliendo las elecciones publicas.

En fin, la pregunta fundamental subsiste, que enfrento a Postel con el resto y amenaza con derrumbar ICANN, sigue siendo la misma:

Deben los usuarios tomar parte en la coordinacion tecnica?.

MAS REFLEXIONES SOBRE EL DOMINIO SET-EZINE.ORG

Ya en la epoca de los hecho y debido a la falta de atencion de gnd en realizar las tareas de editor, consecuencia de una sobrecarga de trabajo y preparacion de viajes de algunos miles de kilometros, SET estaba pasando una epoca bastante mala. Los numeros tardaban en salir debido a que no se respondian a los mensajes y encima se perdian contribuciones al e-zine.

Si ya hay pocas personas dispuestas a invertir su tiempo en escribir algo util para el resto de los mortales, tan solo hace falta que se perdian estas aportaciones para que todo se hunda en breve espacio de tiempo.

De todas formas sigo pensando (y aqui hablo en nombre propio,... un tal madfran) que el responder a las provocaciones de gnd en el IRC con el tentativo de destruccion de todo el trabajo de un conjunto de personas que han contribuido con mejor o peor fortuna al soporte de SET, no me parece en absoluto razonable. A mi modo de ver es como lanzar una bomba contra un autobus, porque el conductor os ha mentado a vuestra madre... despropocionado

EOF

```
-[ 0x0F ]--------------------------------------------------------------------
-[ Extract ]-----------------------------------------------------------------
-[ by SET Staff ]-------------------------------------------------------SET-26-

  La habitual utilidad para extraer ficheros.

<++> utils/extract.c
/*  extract.c by Phrack Staff and sirsyko
 *
 *  (c) Phrack Magazine, 1997
 *      1.8.98 rewritten by route:
 *          - aesthetics
 *          - now accepts file globs
 *      todo:
 *          - more info in tag header (file mode, checksum)
 *  Extracts textfiles from a specially tagged flatfile into a hierarchical
 *  directory strcuture.  Use to extract source code from any of the articles
 *  in Phrack Magazine (first appeared in Phrack 50).
 *
 *  gcc -o extract extract.c
 *
 *  ./extract file1 file2 file3 ...
 */


#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <string.h>
#include <dirent.h>

#define BEGIN_TAG   "<++> "
#define END_TAG     "<-->"
#define BT_SIZE     strlen(BEGIN_TAG)
#define ET_SIZE     strlen(END_TAG)

struct f_name
{
    u_char name[256];
    struct f_name *next;
};

int
main(int argc, char **argv)
{
    u_char b[256], *bp, *fn;
    int i, j = 0;
    FILE *in_p, *out_p = NULL;
    struct f_name *fn_p = NULL, *head = NULL;

    if (argc < 2)
    {
        printf("Usage: %s file1 file2 ... filen\n", argv[0]);
        exit(0);
    }

    /*
     *  Fill the f_name list with all the files on the commandline (ignoring
     *  argv[0] which is this executable).  This includes globs.
     */
    for (i = 1; (fn = argv[i++]); )
    {
```

```
    if (!head)
    {
        if (!(head = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        strncpy(head->name, fn, sizeof(head->name));
        head->next = NULL;
        fn_p = head;
    }
    else
    {
        if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        fn_p = fn_p->next;
        strncpy(fn_p->name, fn, sizeof(fn_p->name));
        fn_p->next = NULL;
    }
}
/*
 *  Sentry node.
 */
if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
{
    perror("malloc");
    exit(1);
 }
fn_p = fn_p->next;
fn_p->next = NULL;

/*
 *  Check each file in the f_name list for extraction tags.
 */
for (fn_p = head; fn_p->next; fn_p = fn_p->next)
{
    if (!(in_p = fopen(fn_p->name, "r")))
    {
        fprintf(stderr, "Could not open input file %s.\n", fn_p->name);
        continue;
    }
    else fprintf(stderr, "Opened %s\n", fn_p->name);
    while (fgets(b, 256, in_p))
    {
        if (!strncmp (b, BEGIN_TAG, BT_SIZE))
        {
            b[strlen(b) - 1] = 0;           /* Now we have a string. */
            j++;

            if ((bp = strchr(b + BT_SIZE + 1, '/')))
            {
                while (bp)
                {
                    *bp = 0;
                    mkdir(b + BT_SIZE, 0700);
                    *bp = '/';
                    bp = strchr(bp + 1, '/');
                }
            }
```

```
                if ((out_p = fopen(b + BT_SIZE, "w")))
                {
                    printf("- Extracting %s\n", b + BT_SIZE);
                }
                else
                {
                    printf("Could not extract '%s'.\n", b + BT_SIZE);
                    continue;
                }
            }
            else if (!strncmp (b, END_TAG, ET_SIZE))
            {
                if (out_p) fclose(out_p);
                else
                {
                    fprintf(stderr, "Error closing file %s.\n", fn_p->name);
                    continue;
                }
            }
            else if (out_p)
            {
                fputs(b, out_p);
            }
        }
    }
    if (!j) printf("No extraction tags found in list.\n");
    else printf("Extracted %d file(s).\n", j);
    return (0);
}

/* EOF */
<-->
*EOF*
```

```
-[ 0x10 ]--------------------------------------------------------------------
-[ Llaves PGP]---------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-26--

PGP <http://www.pgpi.com>

Para los que utilizan comunicaciones seguras, aqui teneis las claves publicas
de algunas de las personas que escriben en este vuestro ezine.

<++> keys/set.asc
Type Bits/KeyID    Date       User ID
pub  2048/286D66A1 1998/01/30 SET <set-fw@bigfoot.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQENAzTRXqkAAAEIAJffLlTanupHGw7D9mdV403141Vq2pjWTv7Y+GllbASQeUMa
Xp4OXj2saGnp6cpjYX+ekEcMA67T7n9NnSOezwkBK/Bo++zd9197hcD9HXbH05zl
tmyz9D1bpCiYNBhA08OAowfUvlH+1vp4QI+uDX7jb9P6j3LGHn6cpBkFqXb9eolX
c0VCKo/uxM6+FWWcYKSxjUr3V60yFLxanudqThVYDwJ9f6ol/1aGTfCzWpJiVchY
v+aWy1i7LxiNyCLL7TtkRtsE/HaSTHz0HFUeg3J5Kiq1VJfZUsn9xlgGJT1Ockaq
HaUBEXbYBPO1YpiAmBMWlapVQA5YqMj4/ShtZqEABRO0GFNFVCA8c2V0LWZ3QGJp
Z2Zvb3QuY29tPokBFQMFEDTRXrSoyPj9KG1moQEBmGwH/3yjPlDjGwLpr2/MN7S+
yrJqebTYeJlMU6eCiql2J5dEiFqgOOQKr5g/RBVn8IQV28EWZCt2CVNAWpK17rGq
HhL+mV+Cy59pLXwvCaebC0/r1nsbxWRcB5rm8KhQJRs0eLx50hxVjQVpYP5UQV7m
ECKwwrfUgTUVvdoripFHbpJB5kW9mZlS0JQD2RIFwpf/Z0ygJL8fGOyrNfOEHQEw
wlH7SfnXiLJRjyG3wHcwEen/r4w/uNwvAKi63B+6aQKT77EYERpNMsDQfEeLsWGr
huymXhjIFET7h/E95IuqfmDGRHoOahfcE7DV4vVvM8wl7ukCUDtAImRfxai5Edpy
N6g=
=U9LC
-----END PGP PUBLIC KEY BLOCK-----
<-->

<-->

<++> keys/paseante.asc
Type Bits KeyID      Created    Expires    Algorithm       Use
pub+ 1024 0xAF12D401 1997-02-19 ---------- RSA         Sign & Encrypt
uid  Paseante <paseante@attrition.org>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAYXR0cml0aW9uLm9yZz6JAJUDBRA4wAATs+ch
/68S1AEBAQkXBAClF2Pv4AGfSOeeWuoANkYrGpJfghH/Difqj8nw1dWkXewBoZSK
69QEo4JvB+UnIi/fhmBVvNWYyL5iWdA/0c3Fx4gKVUDPm2rEnpNbs38ezsyx8VDB
8m0M3vQ4NuFxD8l2VmDUQR6wSNxwNkvp690/Kst4SshGgJ4Gt2mqbKz5Nw==
=Qkzh
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/garrulo.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.0.2

mQDNAzcEBEcAAAEGANGH6CWGRbnJz2tFxdngmteie/OF6UyVQijIY0w4LN0n7RQQ
TydWEQy+sy3ry4cSsW51pS7no3YvpWnqb135QJ+M11uLCyfPoBJZCcIAIQaWu7rH
PeCHckiAGZuCdKr0yVhIog2vxxjDK7Z0kp1h+tK1sJg2DY2PrSEJbrCbn1PRqqka
```

```
CZsXITcAcJQei55GZpRX/afn5sPqMUslOID00cW2BGGSjtihplxySDYbLwerP2mH
u01FBI/frDeskMiBjQAFEbQjR2FycnVsbyEgPGdhcnJ1bG9AZXh0ZXJtaW5hdG9y
Lm5ldD6JANUDBRA3BARH36w3rJDIgY0BAb5OBf91+aeDUkxauMoBTDVwpBivrrJ/
Y7tfiCXa7neZf9IUax64E+IaJCRbjoUH4XrPLNIkTapIapo/3JQngGQjgXK+n5pC
lKr1j6Ql+oQeIfBo5ISnNympJMm4gzjnKAX5vMOTSW5bQZHUSG+K8Yi5HcXPQkeS
YQfp2G1BK88LCmkSggeYklthABoYsN/ezzzPbZ7/JtC9qPK4O7Xmjpm//ni2E10V
GSGkrcnDf/SoAVdedn5xzUhHYsiQLEEnmEijwMs=
=iEkw
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/madfran.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i

mQGiBDcU1qwRBADEG4QNyKmU9llpdZSFMY1JsoQsrj6f0mmxXZjLTpISwYZZkb7d
6EOr/ctaR8fYzqUhRSCbO+/amHWw/Pqb7YcRbXEMT9SjxTcqhlcJXx2ZuQVRgYTW
hSDh8biUZDI8IiI8oosWcj01t3aspDXi77OzjAIqdAuRn4coCp0GSk0fbwCg/5AB
MWuwFDedsPppD7+loLWERnEEAKcQHsuZCoK2yOstfbCezjVZd8tTxP3aI/pxZ14f
mEPS15ONyZKISeeqc7i7QfSBA06L0+ke/B/4l9VxPuv2PVMQi3EeucaWHzq9ntUY
OCugQIPLEdVs5etDA4GLX4Wi0reF+7Ina6O0wQwlHu4Ph4Xn+V/eVU1+/WrPMHeY
69PdA/982Fm8507BCfQcFfaahQHeY0GaOyMZ+1h8+1o6Z4yZDbIEjQzIBvdUtzj7
3ngk/mnIWF4wB26QeSzbzbgneQAw4nJMP2uYjdO9RqsAuozlWR6Aa+KZzCdDDOpo
vma3RWSi+vn3G3QPQUEFBVQOFlt9yfqWf/1z+yCCt7APqi6q8rQdbWFkZnJhbiA8
bWFkZnJhbkBiaWdmb290LmNvbT6JAEsEEBECAAsFAjcU1qwECwMCAQAKCRBym8Cj
IUk+//BaAKCCN/FtWDa1T80mVWNmVdNtTg6mfACgrigD6fHUGCw1x1qruBQ2czUz
8x25Ag0ENxTWrBAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN
/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9
WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0
/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQ
mwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH/2lP9IydeI7B0bZopH99
TOfDnSlqJ6RIhtFv6JHXEIDC+SMPlFj2rOt5VUSAkVNPJqZqczqDPQKrUuCvbqIl
dFUiAPHLdfzjqkGWQnuh1WdAUIIlmOGjXfO3EhrUCW/3zh5hSUmLphDUy5UYtpiY
5OJywzc51c0X1pKtZAZRIQJ9eRaubCq9asBaj4uaMC62kkTe7W6nMsizD+g1uJQZ
8oeyALRc9ytLNqQA1L33wHkp+Uk8vy4Dn1f/1WU4rFibsciWyGobRFk3jofIeZmQ
wevwU2hbxSk3WHup8gA8aFjHA2UXXz2JE6fGuIWH1WdvXGin4SuY718EkC5P9i+E
+omJAEYEGBECAAYFAjcU1qwACgkQcpvAoyFJPv90SwCePCpbXnCGHxOICLOCjOtc
afI4TpEAoIyYVhEq1wgOUMUX8ZUPHLLjsZ20
=k4Yo
-----END PGP PUBLIC KEY BLOCK-----
<-->



<++> keys/nomellames.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 7.0.3 for non-commercial use
<http://www.pgp.com>

mQGiBDygn7YRBADWTdeReufK0QOSlEV2ud3/Y8CqTgzXp4+9sp+l6rO1/L95fOLh
ESEn9yFL+pDuml9i1E8V25GOp5AW7A8x12OmCsYM4EjPicKCqFy5m9wLqKMppDvA
0GO6ZbDh5uGTxhOvFHOEjS1LVjbSm6bdLDXMPuccCCLYSOvyOmlYKi4FVQCg/12p
bdxRmJzyGkgft3Q3ji0jWpMD/27iXI5tOJxg/vDxovcTKarDo5G7rEPaCr+x0tvd
DUqWgDXI6tHMXkElxtprEQmVamfRA6kEz4zq6Iq1yF6kAONUGpGApSwdhsuONCb9
kRIvJiII/D4aMPdiMEVZ9JJeNjtiZCHHv9uunU8RaHLqxBBfrE8NxTz4MOufq6LD
M+ltA/wOsyO56c/MDTbntca0oefDZ1YVyZNnPzKKFv7c+FS+IrqfR0tO4TXPwbiu
vtRGSsbNT6uOOFw0yhBjL8h8cAIkv+y/E+6SU2jYAvmoj82PHlBezXgym50pxUvT
OC4YcxIYmRoCbxB7NLL7Maidg5Udd9yTL4AOwQ0885qeB7TRurQlbm9tZWxsYW1l
cyA8bm9tZWxsYW1lczY2QGhvdG1haWwuY29tPokAWAQQEQIAGAUCPKCftggLAwkI
BwIBCgIZAQUbAwAAAAKCRCPsM+XFXSRQeoiAKDcq//8vm/DF3RA/2W8J+Mp8FL/
```

```
pwCfVCWe+ccDrKd0a3Z0d5jYHpusDF25AgwEPKCfthAIAPZCV7cIfwgXcqK61qlC
8wXo+VMROU+28W65Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh
01D49Vlf3HZSTz09jdvOmeFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscB
qtNbno2gpXI61Brwv0YAWCvl9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFst
jvbzySPAQ/ClWxiNjrtVjLhdONM0/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISn
CnLWhsQDGcgHKXrKlQzZlp+r0ApQmwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVeky
CzsAAgIH90coA44paPVPIamj4rJyM6nnukOB568mNXqHLWpD56Ct8UNi2ZPVpELC
vXAYT6mVDGX1acdwBDNzCJgL3BlflUsH/lX3z6DG6a1sndptIOMsArruHb+cr7Jc
+6b6deyZtK+1tAgv1+h7+c5QA2Hro5Z/m/34F4zZ3yyNHOwPfirC5feGgE4jkKkV
qoA3dT6PAJMfYf15DjHIYX0HsKATVIonXOS585sMDM57qpa5pubbH69eJ0KaMmyq
SEUjg31kwkzDpVQRcBoKtv8RGlSLZe7bY1KeYsR4dNpEHzW6O/7NM1iDliUEKQGD
ksW/vcVVhUnCCcR1PRIFYviW4c3nU4kATAQYEQIADAUCPKCftgUbDAAAAAAKCRCP
sM+XFXSRQVQcAKDY77FGiCYdkNG4o+HQx9irnmL/YgCdE5Z9zSRsp2L2d4DAl8KN
YzmLzBg=
=h5yv
-----END PGP PUBLIC KEY BLOCK-----
<-->
```

```
  ú---------[ ULTIMA ]-------------ú--------------------------------------ú
  |                                |                                      |
  ú---[ ULTIMA NOTA ]--------------ú                                      |
  |                                                                       |
  |  Derechos de lectura:                                                 |
  |     (*)Libres                                                         |
  |                                                                       |
  |  Derechos de modificacion:                                            |
  |     Reservados                                                        |
  |                                                                       |
  |  Derechos de publicacion:                                             |
  |     Contactar con SET antes de utilizar material publicado en SET     |
  |                                                                       |
  | (*)Excepto personas que pretendan usarlo para empapelarnos, para      |
  | ellos 250 Euros, que deberan ser ingresados previamente la cuenta     |
  | corriente de SET, Si usted tiene dudas, tanto para empapelarnos o     |
  | de como pagar el importe, pongase en contacto con SET atraves de las  |
  | direcciones a tal efecto habilitadas.                                 |
  ú-----------------------------------------------------------------------ú
```

mundus vult decipi: ergo decipiatur.
(El mundo quiere ser enganyado: pues que lo sea)

Petronius

SET, - Saqueadores Edicion Tecnica -. Numero #26
Saqueadores (C) 1996-2002

EOF