Protocolo MSN: Compresión de su funcionamiento

(Por Nitz)

Introducción

Hola, soy Nitz, bienvenidos a lo que va a ser una explicación práctica de este protocolo de mensajería instantánea usado por la ¿mayoría? de usuarios. Me voy a centrar en el último protocolo que todavía funciona hasta la fecha: la versión 9.

Bien, este tutorial lo quiero enfocar más que nada para el desarrollo de aplicaciones que utilicen dicho protocolo (bots, clientes, herramientas variadas...)

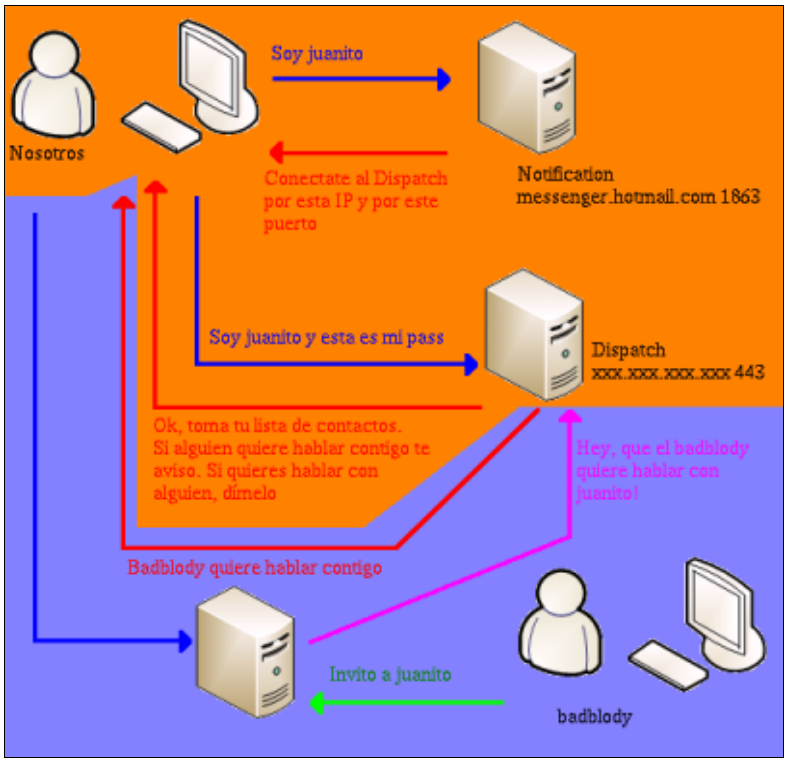
Toda la información la he sacado de:
http://www.hypothetic.org/docs/msn/index.php

Y sin más preámbulos, voy a empezar...

¿Cómo funciona este protocolo?

Para empezar, una sesión de hotmail se basa en 2 servidores, el Notification, el encargado de empezar tu autentificación y el Dispatch, el que continua el login.

El tercer servidor (bueno, tercero, cuarto, quinto...) sirve para establecer conversaciones con los contactos. Cada vez que queramos hablar con alguno, hotmail nos redirigirá a nosotros y a él a un servidor exclusivamente para nosotros :D



Bien, empecemos de una vez por todas...

Iniciando una sesión de telnet...

Bien, para esto necesitaremos... mmm... un **telnet** y... un teclado ;)

Tecleamos en nuestra shell, msdos, consola, butifarra negra, etc:

```
telnet messenger.hotmail.com 1863
```

Ya estamos conectados al primer servidor, procedamos a introducir la versión que utilizamos...
(lo azul es lo que escribimos nosotros; lo rojo, lo que escribe hotmail)

>>VER 1 MSNP9 MSNP8 CVR0
<<VER 1 MSNP9 MSNP8 CVR0

Bien, aquí estamos utilizando el comando VER, se usa para especificar la versión del protocolo msn que utilizaremos, en nuestro caso, la 8 ;)

Una cosa: ¿veis ese "1"? es el TrID ¿Para que se usa? Pues es un sistema de control en hotmail. Cada vez que enviemos un mensaje tenemos que aumentar una unidad ese número. Por ejemplo:

>>COMANDO TRID OPCIONES << Aquí imaginemos que el TrID=1
<<COMANDO TRID OPCIONES << Aquí el servidor nos responde exactamente con el mismo TrID, TrID=1

>>COMANDO 2 OPCIONES << Y vemos que cada vez que enviemos algo, el TrID tiene que ir aumentando ;)
<<COMANDO 2 OPCIONES << Nos responde con el mismo TrID

Los comandos de msn suelen ser de 3 letras, pero bueno, sigamos con lo nuestro...

Ahora tenemos que definir más conceptos, para que hotmail sea capaz de redirigirnos a la versión de msn correspondiente y más actual:

>>CVR 2 0x0C0A winnt 5.1 i386 MSNMSGR 6.0.0602 MSMSGS tu_cuenta_de_hotmail@hotmail.com
<<CVR 2 7.5.0311 7.50311 6.2.0205 http://msgr.dlservice.microsoft.com/download/e/7/5/e75042c3-31c1-4b42-a458-adbc786322fe/Install_MSN_Messenger.EXE http://messenger.msn.com/es

Mmm... vaya ristra de datos... Bien, empecemos a explicarlos: el comando que enviamos, CVR, es el encargado de decirle a hotmail la versión de nuestro SO, el procesador que usamos, la versión del CLIENTE msn que utilizamos (el cliente, y NO la versión del protocolo).

Osea que en ese comando podemos poner lo que nos salga, que no importa, incluso si estamos en Linux podemos poner que usamos un WinXP, que da igual. Por cierto, poned vuestra cuenta de hotmail y no esa que he puesto de ejemplo ;)

A continuación nos dice que nos bajemos una versión más actual, y nos da el link y todo ;) pero nosotros somos unos 'pofesionales' que no necesitamos ninguna versión nueva, osea que pasamos de lo que nos diga como de la "caca" :P

Bien, sigamos...

>>USR 3 TWN I tu_cuenta_de_hotmail@hotmail.com
<<XFR 3 NS 207.46.106.35:1863 0 207.46.104.20:1863

El comando USR nos identifica junto con "TWN I" y nuestra cuenta de hotmail. Después el servidor nos responde dándonos la IP del nuevo servidor a dónde conectarnos, el puerto, un valor nulo (el 0) y la IP y el puerto del servidor actual donde estamos conectados.

Bien, pues nos conectamos a ese servidor:

```
telnet 207.46.106.35 1863
```

Autentificandonos...

Bien, ahora que ya nos hemos conectado:

>>VER 4 MSNP9 MSNP8 CVR0 <---- Volvemos a lo de antes, la identificación de versiones

```
<<VER 4 MSNP9 MSNP8 CVR0
>>CVR 5 0x0409 win 4.10 i386 MSNMSGR 5.0.0544 MSMSGS
tu_cuenta_de_hotmail@hotmail.com
<<CVR 5 6.0.0602 6.0.0602 1.0.0000
http://download.microsoft.com/download/8/a/4/8a42bcae-f533-4468-b871-
d2bc8dd32e9e/SETUP9x.EXE http://messenger.msn.com
```

Bien, como vemos, volvemos a identificar nuestra versión del protocolo, del cliente y de la ropa interior :P

Continuemos con la identificación del usuario...

```
>>USR 6 TWN I tu_cuenta_de_hotmail@hotmail.com
<<USR 5 TWN S
lc=1033,id=507,tw=40,fs=1,ru=http%3A%2F%2Fmessenger%2Emsn%2Ecom,ct=1139411464,kp
p=1,kv=7,ver=2.1.6000.1,rn=NfNw1dnJ,tpf=773901fc3222b6a78f24f3f9955ca7c9
```

Aquí nos está "etiquetando", nos da una especie de cookie para identificarnos en el próximo servidor, todos esos campos (lc, id, etc) son los que harán falta luego. Ahora debemos conectarnos al próximo servidor de autentificación **SIN DESCONECTARNOS DE ESTE**:

```
telnet login.passport.com 443
```

Y enviar todo esto:

```
>>GET /login2.srf HTTP/1.0
Accept: */*
Host: login.passport.com
User-Agent: loquesea
Authorization: Passport1.4
OrgVerb=GET,OrgURL=http%3A%2F%2Fmessenger%2Emsn%2Ecom,sign-
in=tu_cuenta_de_hotmail,pwd=tu_password,lc=1033,id=507,tw=40,fs=1,ru=http%3A%2F%
2Fmessenger%2Emsn%2Ecom,ct=1139411464,kpp=1,kv=7,ver=2.1.6000.1,rn=NfNw1dnJ,tpf=
773901fc3222b6a78f24f3f9955ca7c9
```

Esta parte es la encargada de identificarse ante el servicio de autentificación de hotmail, dando la cuanta de usuario en codificación url (fijaros en que la @ es sustituida por %40) y el password **EN FORMATO CLARO.** Fijaros también en que hay que rellenar todos los datos que nos ha enviado el antiguo servidor para verificar que realmente somos nosotros.

Mmm... Eso del password en formato claro me está dando la idea de meter un sniffer y empezar a capturar tráfico a destajo... Bueno, esto ya os lo dejo a vosotros ;)

Por cierto, si esto está en formato claro es única y exclusivamente porque nos estamos autentificando sin SSL. Esta opción la puedes deshabilitar en tu cliente de msn, pero lo normal es que venga activada por defecto :P

Y el servidor a todo esto nos respondería:

```
<<HTTP/1.1 200 OK
Connection: close
Date: Sat, 04 Feb 2006 13:05:47 GMT
Server: Microsoft-IIS/6.0
PPServer: PPV: 30 H: BAYPPLOGN3A17 V: 0
Content-Type: text/html; charset=iso-8859-1
Expires: Sat, 04 Feb 2006 13:04:47 GMT
Cache-Control: no-cache
Pragma: no-cache
P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"
Set-Cookie:
```

```
PPAuth=ATfnpiMQtylf6P507v3NaCN2A3ihR!NBmSQpTYqL2OMEi6hJJOla!R!tUimrfFGFOmSu*MKLl
6s9T5VN*hFYc58VX2S*kRYLc0d0keCOeCfjkkfxsjU*HNU4LPCPCVVixqCySiGxYSqV0*kW4gLUxpqLb
5gxpX3SoJbT0Q2Y6HqmBSzirQ$$; domain=.passport.com;secure= ;path=/;HTTPOnly=
;version=1
Set-Cookie: PPLState=1; domain=.passport.com;path=/;HTTPOnly= ;version=1
Set-Cookie: MSPVis=507;domain=.passport.com;path=/
Authentication-Info: Passport1.4 da-status=success,from-
PP='t=7VO2GTOZSCzUXz0u!YAHOTdfatJTMx4gRkLO7IIzamtxSk0wB8!9JRX4ru0Tgh2Eu7l7S*33Mm
8QKD4LGXcjyjgs9NOcj6DoSlaX4UkfFKRlA71EtiuJrc!9RtJAVuljEq&p=74Wlr0gILBOcxOYrUP5x7
DqGO4GysnPAyb4yJ5AkfbtgaOLP5BxeMUTn5JlEzsbCdFG8A3o*VTqRpg5LiJvroLFNtNZE9JkC!7*wL
gAun1FiVjUbNDZlhbt68oD!MY1UqRz68EdyQCG5UA*jNFUrM8icKoH2mj1dDI1SyLIEEig00OIlYYjtV
l4I*Fgy1EZCZxHtAR6ZIdk1s$',ru=http://messenger.msn.com
Connection: Keep-Alive
Content-Length: 0
```

¡Fijaros en ese “t=...”! Hay que apuntar ese valor porque ahora hay que enviárselo **al servidor de antes, el que he dicho que no cerraras.**

Bien, se lo enviamos y...

```
>>USR 7 TWN S
t=7VO2GTOZSCzUXz0u!YAHOTdfatJTMx4gRkLO7IIzamtxSk0wB8!9JRX4ru0Tgh2Eu7l7S*33Mm8QKD
4LGXcjyjgs9NOcj6DoSlaX4UkfFKRlA71EtiuJrc!9RtJAVuljEq&p=74Wlr0gILBOcxOYrUP5x7DqGO
4GysnPAyb4yJ5AkfbtgaOLP5BxeMUTn5JlEzsbCdFG8A3o*VTqRpg5LiJvroLFNtNZE9JkC!7*wLgAun
1FiVjUbNDZlhbt68oD!MY1UqRz68EdyQCG5UA*jNFUrM8icKoH2mj1dDI1SyLIEEig00OIlYYjtVl4I*
Fgy1EZCZxHtAR6ZIdk1s$

<<USR 7 OK tu_cuenta_de_hotmail@hotmail.com tu_nick_actual 1 0
<<MSG Hotmail Hotmail 506
MIME-Version: 1.0
Content-Type: text/x-msmsgsprofile; charset=UTF-8
LoginTime: 1139058348
EmailEnabled: 1
MemberIdHigh: 425982
MemberIdLow: -2047945872
lang_preference: 3082
preferredEmail:
country: ES
PostalCode:
Gender:
Kid: 0
Age:
BDayPre:
Birthday:
Wallet:
Flags: 1073742915
sid: 507
kv: 7
MSPAuth:
7VO2GTOZSCzUXz0u!YAHOTdfatJTMx4gRkLO7IIzamtxSk0wB8!9JRX4ru0Tgh2Eu7l7S*33Mm8QKD4L
GXcjyjgs9NOcj6DoSlaX4UkfFKRlA71EtiuJrc!9RtJAVuljEq
ClientIP: WEEEE-ESTA-ES-MI-IP
ClientPort: 31305
```

Dios, vaya rollazo, pero lo único que nos interesa son los dos últimos mensajes, que es donde te da toda la información correspondiente a tu cuenta.

En el primer mensaje te dice:

```
USR 7 OK tu_cuenta_de_hotmail@hotmail.com tu_nick_actual 1 0
```

¿No hace falta dar explicaciones, verdad? Nos dice más que nada el nick que tenemos actualmente ;)

Ahora es cuando nos da la información sobre la lista de contactos:

>>SYN 8 0
<<SYN 8 13 5 4

Le enviamos al servidor el comando correspondiente para que nos dé la lista de contactos. Como parámetro a nuestro SYN le ponemos versión de la lista de contactos que usamos por última vez en nuestro cliente (MSN messenger tiene un registro para agilizar el inicio de sesión)

Para el que no lo haya entendido bien, voy a hacer una breve explicación:

Nuestra lista de contactos al crear nuestra cuenta de hotmail es la versión 0, ya que no la hemos modificado, pero en el momento que añadamos, borramos, editemos, etc algún contacto, el número de versión aumentará.

Imaginemos que nuestra lista se encuentra en la versión 5. Tenemos estos contactos

- woody
- noitami
- HeNuX
- Addex
- Manu_barcelona

Bien, ahora vamos a añadir uno más: kaiszz.
Nuestra lista automáticamente se actualizaría a la versión 6, quedando así:

- woody
- noitami
- HeNuX
- USHER
- Manu_barcelona
- kaiszz

Nosotros en nuestro comando SYN hemos utilizado como parámetro el 0, así el servidor nos dará la lista COMPLETA de nuestros contactos. ¿Qué hubiera pasado si hubiéramos puesto el 5?
Pues que el servidor sólo nos hubiera informado de que tenemos el contacto kaiszz en nuestra lista.

¿Por qué tenemos la opción de informarnos sólo de los últimos cambios?
Pues porque el cliente MSN Messenger guarda nuestra lista de contactos en nuestro PC, para así luego, agilizar la conexión pidiendo solo los últimos cambios y añadiéndolos a la lista local.

Analicemos los parámetros de respuesta que nos ha mandado el servidor:

13: la versión actual de la lista. Hemos hecho 13 cambios desde que creamos la cuenta de hotmail.
5: el número de grupos que tenemos creados en nuestra lista (amigos, familiares, chicas-fáciles :D)
4: el número de contactos que tenemos agregados

Ahora nos dará ya la apreciada lista:

<<GTC A
<<BLP AL
<<PRP MBE N
<<PRP WWE 0

Sinceramente, ni idea de que es todo esto. No he conseguido obtener información de ningún tipo sobre estos términos, pero creo que andan relacionados con las 4 listas de usuarios que existen en cada cuenta de hotmail.

Una aclaración sobre las "listas":

Hotmail usa 4 listas de usuarios para cada cuenta, que se clasifican a su vez en 2 tipos:

Listas de contactos:

- FL: Forward List, la lista de tus contactos, vamos la que vemos en nuestro cliente de msn
- RL: Reverse List, la lista de usuarios que te tienen agregado, los que te tienen en su propia FL
- AL: Allow List, lista de usuarios que te pueden "ver", los que tienes como "admitidos"
- BL: Block List, la lista de usuarios que no quieres que te vean, los "no admitidos"

Bueno, pero lo que viene ahora es lo que nos interesa ;)

<<LSG 0 Frikis 0
LSG 1 Los%20que%20la%20arman 0
LSG 2 Con%20fundamento 0
LSG 3 Admins 0
LSG 4 Jugones 0

Esta lista nos dice los grupos que tenemos creados. Como podemos ver, está en codificación url, como todos los nicks, sustituyendo los espacios por "%20". también observamos que a cada grupo de la un índice (0, 1, 2, 3 y 4) para identificarlos más adelante... ¡Ah! y ese valor "0" es un valor nulo, vamos, que está por estar ;)

Ahora nos da la información de los nicks:

<<LST woody@hotmail.com woody 3 3
<<LST noitami@hotmail.com noitami 3 0
<<LST HeNuX@hotmail.com HeNuX 3 4
<<LST carlitos@hotmail.com USHER 3 0,1,2,4
<<LST manu@hotmail.com Manu%20Barcelona 3 1
<<LST kaiszz@hotmail.com kaiszz 3 2

Bien, empecemos la explicación:

Vemos que por cada contacto nos ofrece la siguiente sintaxis: LST Email Nick lista grupo

Sobre ese parámetro, "lista", nos informa sobre en qué lista tenemos a ese contacto. Su explicación es bastante compleja, ya que puede adoptar varios valores, y esto ya se aleja un poco del propósito de este artículo, que es mostrar el protocolo para su uso en aplicaciones. Si te curras un cliente, no necesitarás estos datos excepto en casos muy avanzados.

Entonces vemos que woody pertenece al grupo 3 (admins), noitami al 0 (frikis), HeNuX pertenece al grupo 4 (jugones), Manu Barcelona al 1 (los que la arman) y kaiszz al 2 (con fundamento).

¿Todo claro?

Ahora vemos una excepción, USHER, que pertenece al 0,1,2 y 4. Esto quiere decir que lo tenemos "metido" en los grupos Frikis, Los que la arman, Con fundamento y Jugones. Osea, que a un mismo usuario lo podemos embutir en tantos grupos como

queramos ;)

Ahora que ya tenemos nuestros contactos repartidos, toca poner nuestro estado en "en línea", o "al teléfono" o a lo que sea. Para hacer esto usaremos el comando "CHG" junto a un parámetro que especifique el estado al que deseamos pasar. La sintaxis es la siguiente:
CHG TrID PARAMETRO

Veamos los estados que podemos adoptar:

- En línea: el parámetro será "NLN"
- Desconectado: el parámetro será "FLN"
- Invisible: el parámetro será "HDN". Todos los contactos te verán como desconectado, pero estarás conectado
- Inactivo: el parámetro será "IDL"
- Ausente: el parámetro será "AWY"
- Vuelvo enseguida: el parámetro será "BRB"
- No disponible: el parámetro será "BSY"
- Al teléfono: el parámetro será "PHN"
- Salí a comer: el parámetro será "LUN"

Así que vamos a empezar la conexión con el estado, por ejemplo, "No disponible". Ahora tocaría introducir:

```
>>CHG 9 BSY
<<CHG 9 BSY 4096
```

Si quisieramos iniciar sesión con el estado "El línea" a secas, pues:

```
>>CHG 9 NLN
<<CHG 9 NLN 4096
```

Mmm... Parece que si que ha funcionado el cambio, ¿no? Este número, el 4096 no es más que otro valor nulo, no quiere decir nada ;)

Ahora que ya todos nuestros contactos saben que estamos vivos, el servidor nos mandará automáticamente una lista de la gente que se encuentra online en este momento.

```
<<ILN 9 NLN woody@hotmail.com woody 1342558260
%3Cmsnobj%20Creator%3D%22woody%40hotmail.com%22%20Size%3D%2220488%22%20Type%3D%2
23%22%20Location%3D%22TFR96.dat%22%20Friendly%3D%22AAA%3D%22%20SHA1D%3D%2299kFrj
GuAygMvYcNZO9GSai%2FyWA%3D%22%20SHA1C%3D%22HiLMN3YyZREw7F9DX7Vk2Qeijsk%3D%22%2F%
3E
```

Uf, esto parece muy complicado, vamos a analizarlo:

- ILN: respuesta que nos informa que está conectado
- 9: el TrID ;)
- NLN: Dice que se encuentra "En línea"
- woody@hotmail.com: El email (cuenta) del contacto
- woody: El nick que utiliza actualmente.
- 1342558260...: Esto ya es información aparte, referente al blog, perfil y imagen para mostrar del contacto

Y no tenemos solo a woody online, sino que hay más gente:

```
<<ILN 9 NLN woody@hotmail.com woody 1342558260...
<<ILN 9 BSY noitami@hotmail.com JosE 3523524670...
<<ILN 9 IDL USHER@hotmail.com USHER%20-%20weeeeee 8493587345...
```

Como se puede ver, me he ahorrado todo ese código referente al blog, al perfil y estas historias. Bien, esto nos dice que están online woody@hotmail.com (woody), noitami@hotmail.com (JosE) y carlitos@hotmail.com (USHER - weeeeee).

Pero como se puede apreciar, noitami está en "BSY" (no disponible) y USHER en "IDL" (inactivo, vamos, que hace rato que no hace nada).

Después de toda esta lista de contactos, nos aparecerá información extra, como puede ser, el estado de nuestra bandeja de entrada.

```
<<MSG Hotmail Hotmail 219
MIME-Version: 1.0
Content-Type: text/x-msmsgsinitialemailnotification; charset=UTF-8

Inbox-Unread: 0
Folders-Unread: 8
Inbox-URL: /cgi-bin/HoTMaiL
Folders-URL: /cgi-bin/folders
Post-URL: http://www.hotmail.com
```

Aquí lo único importante que deberíamos ver, sería el "Inbox-Unread", que nos dice la cantidad de emails sin leer que tenemos en nuestra bandeja de entrada y también "Folders-Unread", que nos dice los emails no-leidos de nuestras carpetas en nuestra cuenta.

Ya está todo listo!!!

Abriendo nuestros horizontes: entablamos una conversación

Bueno, llevamos aquí tres cuartos de hora y todavía no hemos ni saludado a la peña.

Para empezar, se pueden establecer dos tipos de conversación: iniciándola tú o que te invite otro contacto.

A partir de ahora tendréis que sustituir el TrID por el respectivo valor, ya que estos comandos los podemos poner el cualquier parte de la sesión.

Comenzamos nosotros:

Enviamos a nuestro servidor el comando:

```
>>XFR TrID SB
<<XFR TrID SB 65.54.171.44:1863 CKI 406536365.21820633.24452208
```

Bien, la respuesta del servidor nos da la información que necesitamos:

- 65.54.171.44: La ip del servidor donde estableceremos la conversación
- 1863: El puerto por donde debemos establecerla
- 406536365.21820633.24452208: un número aleatorio que debemos recordar ;)

Ok, todo correcto, abrimos otro telnet y nos conectamos al servidor **Switchboard**, el tercer y último servidor, dónde estableceremos nuestra conversación.

```
telnet 65.54.171.44 1863
```

Y ahora que estamos conectados debemos identificarnos para que el servidor nos reconozca ¡Pero tranquilos! No hay que superar ningún desafío para la contraseña ni nada por el estilo. Lo único que hay que hacer es justo al conectarse enviar el siguiente comando:

```
>>USR 1 tu_cuenta_de_hotmail@hotmail.com 406536365.21820633.24452208
<<USR 1 OK tu_cuenta_de_hotmail@hotmail.com tu_nick
```

¿Que hemos mandado?
1: es el TrID, observemos que hemos empezado una nueva "tanda" desde 1 ya que hemos cambiado de servidor. PERO OJO, ahora podemos poner el número 1 **siempre**

406536365.21820633.24452208: es el número que hemos dicho que recordaras antes, ¿no?. Esto es una medida de seguridad que usa hotmail para no "apropiarte" de conversaciones ajenas.

Esta protección la podríamos saltar si estuviéramos en la misma red local que la víctima. Montamos un sniffer, capturamos el tráfico y nos hacemos con el número y la IP del servidor, nos conectamos, introducimos el email de la víctima y su número. Ya está, tenemos una conversación con un amigo de la víctima ;)

Pero como este articulo no está orientado al hacking de hotmail, sigamos con lo nuestro :P

Ahora tenemos que invitar a nuestro contacto a la conversación, lo hacemos con el comando CALL:

```
>>CAL 1 carlitos@hotmail.com
<<CAL 1 RINGING 406536365
<<JOI carlitos@hotmail.com USHER%20-%20weeeeee
```

Bien, podemos ver que invitamos a USHER (carlitos@hotmail.com) y la respuesta del comando es correcta, lo estamos llamando. A continuación vemos que se une a nuestra conversación (la respuesta del JOI).

Segundo método, nuestro contacto nos invita a nosotros

Estamos tan tranquilos teniendo una sesión de msn cuando USHER nos invita a una conversación. ¿Que hacemos?
Bien, para empezar, nos llegará un mensaje de este tipo:

```
<<RNG 217144 207.46.2.159:1863 CKI 1139406941.12018 carlitos@hotmail.com
USHER%20-%20weeeeee
```

Vemos que nos dan una IP (207.46.2.159) y un puerto (1863). Esta es la IP del servidor al que nos deberemos conectar para establecer nuestra conversación. Y ese número, el primer número aleatorio de control (217144) junto con el otro, el segundo (1139406941.12018) lo apuntamos en un papel ;)

Establecemos la conexión con el nuevo host:

```
telnet 207.46.2.159 1863
```

Ahora enviamos:

```
>>ANS 1 tu_cuenta_de_email@hotmail.com 1139406900.12018 217144
<<IRO 1 1 1 carlitos@hotmail.com USHER%20-%20weeeeee
<<ANS 1 OK
```

En el primer comando enviamos nuestra cuenta de email + el segundo número aleatorio de control + el primer número aleatorio de control.
Entonces el servidor nos responde con la gente que está actualmente en este servidor (solo USHER, por supuesto) y un mensaje de notificación que nos informa de que todo ha ido correctamente.

Ahora intentamos hablar ;)

Bueno, ahora que ya está la fiesta montada, digamos nuestro primer "Hola" ;)

```
>>MSG 1 N 135
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=Verdana; EF=; CO=800000; CS=0; PF=22

jander macander
```

Buf... por donde empezar...

- MSG 1 N 135: esto es el comando en sí. El número ese que veis (135) es la cantidad de letras que contendrá nuestro mensaje. ¡Pero cuidado! Nuestro mensaje no es solo "jander macander", sino que es **todo lo que viene después de esta linea que estamos analizando.**
- MIME-Version: 1.0 /// Content-Type: text/plain; charset=UTF-8: Esto siempre es igual, es la descripción de lo que queremos enviar, no hace falta cambiarlo.
- X-MMS-IM-Format: FN=Verdana; EF=; CO=800000; CS=0; PF=22: Esto tiene más de miga...
    - FN: El tipo de fuente que usamos. En nuestro caso "Verdana", pero puede ser también "Times%20New"
    - EF: Efectos que queramos para nuestra fuente. Si queremos poner cursiva, escribimos "EF=I", si queremos negrita "EF=B", subrayada "EF=S". Pero también se pueden combinar, así que si queremos una fuente en negrita y cursiva podemos poner "EF=BI" o "EF=IB", da lo mismo.
    - CO: El color que queramos en hexadecimal. Si queremos el negro ponemos "CO=000000", el blanco "CO=ffffff", etc...
    - CS: La codificación de caracteres que queremos utilizar. Aquí expongo una tabla de todos los existentes:

0 - ANSI_CHARSET
ANSI characters
1 - DEFAULT_CHARSET
Font is chosen based solely on name and size. If the described font is not available on the system, Windows will substitute another font.
2 - SYMBOL_CHARSET
Standard symbol set
4d - MAC_CHARSETLT
Macintosh characters
80 - SHIFTJIS_CHARSET
Japanese shift-JIS characters
81 - HANGEUL_CHARSET
Korean characters (Wansung)
82 - JOHAB_CHARSET
Korean characters (Johab)
86 - GB2312_CHARSET
Simplified Chinese characters (Mainland China)
88 - CHINESEBIG5_CHARSET
Traditional Chinese characters (Taiwanese)
a1 - GREEK_CHARSET
Greek characters
a2 - TURKISH_CHARSET
Turkish characters
a3 - VIETNAMESE_CHARSET
Vietnamese characters
b1 - HEBREW_CHARSET
Hebrew characters
b2 - ARABIC_CHARSET
Arabic characters
ba - BALTIC_CHARSET
Baltic characters
cc - RUSSIAN_CHARSET_DEFAULT
Cyrillic characters
de – THAI_CHARSET
Thai characters
ee - EASTEUROPE_CHARSET
Sometimes called the "Central European" character set, this includes diacritical marks for Eastern European countries
ff - OEM_DEFAULT

Depends on the codepage of the operating system

- PF: Esto espefica la categoría del tipo de fuente de FN, es decir, podemos poner "Times%20New" con el tipo "Roman". Aquí os pongo una tabla de los posibles valores:

```
0_ - FF_DONTCARE
    Specifies a generic family name. This name is used when information about a
font does not exist or does not matter. The default font is used.
1_ - FF_ROMAN
    Specifies a proportional (variable-width) font with serifs. An example is
Times New Roman.
2_ - FF_SWISS
    Specifies a proportional (variable-width) font without serifs. An example
is Arial.
3_ - FF_MODERN
    Specifies a monospace font with or without serifs. Monospace fonts are
usually modern; examples include Pica, Elite, and Courier New.
4_ - FF_SCRIPT
    Specifies a font that is designed to look like handwriting; examples
include Script and Cursive.
5_ - FF_DECORATIVE
    Specifies a novelty font. An example is Old English.

_0 - DEFAULT_PITCH
    Specifies a generic font pitch. This name is used when information about a
font does not exist or does not matter. The default font pitch is used.
_1 - FIXED_PITCH
    Specifies a fixed-width (monospace) font. Examples are Courier New and
Bitstream Vera Sans Mono.
_2 - VARIABLE_PITCH
    Specifies a variable-width (proportional) font. Examples are Times New
Roman and Arial.
```

- jander macander: Esto como podréis suponer, es el mensaje que hemos escrito ;)

¿Ha costado verdad? Pero si automatizamos nuestra aplicación para que lo haga él solo, todo va de perlas ;)

Bueno, ahora nos tiene que responder nuestro contacto, que ya ha leído nuestro mensaje, pero para eso **tiene que teclear su mensaje antes**:

```
<<MSG carlitos@hotmail.com USHER%20-%20weeeeee 93
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: carlitos@hotmail.com
```

Vemos que el Content-Type nos dice que es un mensaje de control, y nos muestra una línea más abajo que USHER está escribiendo un mensaje (¿Recordáis esos mensajes debajo de la ventanita del msn?).

Por cierto, fijaros en ese 93 de la primera línea, que es la cantidad de letras que tiene ese mensaje.

Y ahora por fin, nuestro amigo USHER contesta:

```
<<MSG carlitos@hotmail.com USHER%20-%20weeeeee 139
MIME-Version: 1.0
```

Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=Lucida%20Console; EF=B; CO=db000; CS=0; PF=31

juguijugui

Venga, no explico lo de las cabeceras (estilo de fuente y demás historias) porque ya lo he dicho antes :P
Solo digo que USHER nos ha respondido "juguijugui" :D

De repente a USHER le da la neura y nos cierra la ventana de conversación de su MSN Messenger, osease, que abandona el servidor de conversación, abandona el Switchboard.

Entonces recibimos nosotros:

<<BYE sherlock_holmes1989@hotmail.com

Si nosotros cerrásemos nuestro telnet, a carlos también le enviarían ese mensaje.

Acabado ya esta sección, pasemos a unos aspectos secundarios de una típica sesión de msn...

Otros temas relacionados

PING

En repetidas ocasiones el servidor notification (el segundo), nos enviará pings. Tendremos que responderlos. Aquí pongo un ejemplo:

<<CHL 0 51623305299613071178

Nos ha mandado un parámetro aparte, que se constituye de un número aleatorio, en este caso, el 51623305299613071178.
Ahora con este número tendremos que realizar una operación especial, “pegarlo” junto a una cadena específica que siempre es la misma y codificarlo a MD5 ;)

La cadena es: “Q1P7W2E4J9R8U3S5”

51623305299613071178 + Q1P7W2E4J9R8U3S5 = 3471fc1d6961c55254d490bc67637f1c

o lo que es lo mismo,
5162330529961307117 8Q1P7W2E4J9R8U3S5 = 3471fc1d6961c55254d490bc67637f1c

Pasar a MD5 una cadena
En linux es bastante facil pasar una cadena a MD5, creas un archivo de texto plano con la cadena que quieras dentro de él y después lanzas el comando

```
md5sum archivo
```

En windows tienes que usar programas externos, o consultar webs que te lo hacen online, como esta: http://kodesoft.net/md5/md5.php

Y se lo enviamos al servidor junto a unos parámetros **que nunca se han de modificar**.

Esto realmente no es así, se pueden modificar y poner otros parámetros, funcionarán igual, pero no los expongo para no complicar la cosa ;)

Lo dicho, enviamos:

>>QRY TrID msmsgs@msnmsgr.com 32 <<Aquí hacemos un salto de línea!

3471fc1d6961c55254d490bc67637f1c **<<Pero aquí ya no hay que hacerlo, recordadlo!**
<<QRY TrID

Por cierto, cuando
Ese "QRY" nos dice que todo ha salido bien ;) hemos respondido correctamente al ping.

CAMBIO DE ESTADO: de nuestra sesión

Si quisieramos cambiar de estado a no-disponible sólo tendríamos que introducir:

>>CHG TrID BSY
<<CHG TrID BSY 0

Claro que en BSY podemos poner cualquier abreviación de las que he comentado antes (Ausente: AWY ...).

CAMBIO DE NICK

Enviamos:

>>REA TrID tu_cuenta_de_hotmail@hotmail.com nuevo_nick
<<REA TrID 1 tu_cuenta_de_hotmail@hotmail.com nuevo_nick

Recordad que el nick debe estar escrito en formato url ("mi nombre" = "mi%20nombre")

CAMBIO DE ESTADO Y DE NICK: de un contacto

Nos llegaría el comando en cualquiera de los dos casos:

<<NLN BSY carlitos@hotmail.com Este%20es%20mi%20nuevo%20nick!!! 1342492724...

- En BSY estaría el estado correspondiente de nuestro contacto. A no ser que sea FLN, que sustituiría toda la cadena "NLN BSY" quedando sólo como "FLN"
- En carlitos@hotmail estaría la cuenta de correo de nuestro contacto (obvio, no?)
- En Este%20es%20mi%20nuevo%20nick!!! estaría el nuevo nick del contacto ;)
- Y por último, en 1342492724... correspondería a toda la información sobre la foto para mostrar, el perfil, etc.

Despedida

Bueno, esto ha sido todo, el curro de toda una semana ;)
Espero que uséis este manual para crear todo tipo de aplicaciones, que este protocolo da para mucho ;)

Agradecimientos a kaiszz y woody porque sin su ayuda no hubiera podido corregir un error (2 más bien) que tenia este documento ;)

Saludos!
Nitz (www.ZiberZone.net)