La delgada barrera que separa los códigos maliciosos ilegales de los legales (Adware y Spyware)

Fuente: André Goujon Maucher - agoujonm(arroba)gmail(punto)com

Fecha de Publicación: 01-10-2005

Últimamente cuando contratamos con casi cualquier ISP una línea de Internet de Adsl, el router y un CD con la configuración suelen formar parte de su paquete de bienvenida, además, el router suele ser Wifi porqué en la actualidad casi todos queremos vernos libres de las ataduras de los cables, y también porqué casi todos tenemos, además del equipo de sobremesa, un portátil con el que también nos conectamos a Internet.

Sin embargo, ese vernos libres de ataduras, conectando nuestros equipos a la red sin cables, a veces nos puede costar que si no la tenemos convenientemente segura, nuestros vecinos se abonen a ella, limitando de ese modo nuestra velocidad.

En este texto vamos a tratar de asegurar nuestra red Wifi al máximo posible, aunque por razones obvias no podemos poner capturas de pantalla puesto que las diversas opciones, dependiendo de cada router, las encontraremos en un sitio u otro. No obstante, con estas indicaciones y el manual de nuestro router que siempre suele venir en el paquete, será fácil asegurar la red.

Pero primero una reflexión: ¿de verdad necesitamos una conexión Wifi?
Si nuestro router está situado, como es casi lo habitual, al lado del PC es mucho más fiable, usar el cable Ethernet que la comunicación Wifi, y ésto, además de por seguridad, por una razón de velocidad, las conexiones por cable Ethernet transmiten a una velocidad (Ethernet 10/100) de 100 Mbps, mientras que las transmisiones inalámbricas en la actualidad son (con el Standard 802.11g que es el más común hoy en día) a 54 Mbps.

Por tanto, si la conexión la podemos establecer vía ethernet, mejor usar ésta, pero si a pesar de todo queremos tener establecida una red Wifi en casa, unos puntos a tener en cuenta que mejorarán la seguridad.

- Cambiar la contraseña que viene por defecto en nuestro router
- Modificar el SSID que viene configurado por defecto
- Modificar el canal
- Desactivar la difusión del nombre de la red (broadcast del SSID)
- Cifrar la red usando WPA o si el modelo de router lo permite WPA2 (y usando contraseñas seguras)
- Activar el filtrado por direcciones MAC (Identificador hexadecimal único de cada dispositivo)
- Desactivar el servidor DHCP (asignaremos las direcciones IPs manualmente)
- Cambiar la clave de cifrado de forma regular

Cuando no estemos usando la red, apagar el router

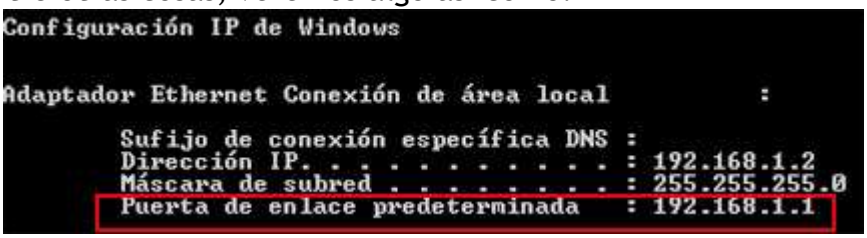
Y por supuesto, y si nuestros conocimientos nos lo permiten, usar rangos de direcciones IPs limitados por Subnettig.

Antes de empezar, a modificar opciones wireless de nuestro router para asegurar la red, debemos tener en cuenta que todas estas modificaciones han de hacerse conectado UNICAMENTE vía cable Ethernet, la razón es por otra parte lógica, es casi seguro que al realizar alguna modificación, perdamos la conexión.
Otra recomendación es que anotéis todas las modificaciones que se hagan y en que apartado se encuentran.

Para acceder a nuestro router vía navegador, tan sólo hemos hemos de saber la dirección ip con la que comunicarnos, y eso lo conseguimos (si no la sabemos de antemano) con estas instrucciones:

- Pulsamos inicio
- Ejecutar
- Escribimos cmd, y en la pantalla que nos aparece tecleamos ipconfig

Allí entre otras cosas, veremos algo así como:



Puerta de enlace predeterminada y una dirección que suele ser 192.168.1.1, bien pues si ponemos en nuestro navegador y pulsamos enter, nos encontraremos que hemos entrado en las entretelas de nuestro router.

Ahora veamos punto por punto como se hace para asegurar nuestra red:

Cambiar la contraseña por defecto del router:
Todos suelen salir de fábrica con un password por defecto, es muy fácil encontrar bastantes páginas en Internet donde hay listas con los password de cada marca de router, por eso una de las primeras medidas pasa por cambiarlo.
Eso suele estar en el apartado **System Tools/Admin password**, aquí ponemos la clave por defecto y en el apartado **New password** ponemos la nueva, recordar un password de al menos 10 dígitos, compuesto de números, letras y caracteres especiales. Naturalmente ese password debemos anotarlo, pues si llegado el momento no lo recordamos nos tocará resetear el router y volver a configurarlo desde cero.

Después de cada modificación, debemos pulsar Apply, Save o Salvar si está en español para guardar los cambios

Modificar el SSID (Service Set IDentifier)
O nombre de nuestra red wifi, es un código con un máximo de 32 caracteres alfanuméricos, todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.
Se suele encontrar en el apartado **Wireless Settigns**, normalmente nos encontraremos o bien el nombre de nuestro router, o el de nuestro Isp, lo moficaremos por otro que no sea el habitual. La razón es lógica, estamos ocultando el nombre de nuestra red wifi, por tanto si desconocen a quien hay que atacar, ya le estamos poniendo alguna dificultad.

Modificar el Canal
Al igual que el SSID, lo encontramos en **Wireless Settings** podemos usar cualquier canal de los que nos aparezca en el desplegable, a no ser que nuestro proveedor nos indique lo contrario.

Desactivar broadcast del SSID (Service Set IDentifier)
O lo que es lo mismo, que no haga público el nombre de nuestro SSID (nombre de nuestra red wifi) que el router difunde y que cualquier sistema que busque una conexión encontrará.
También lo encontramos en el mismo apartado, tan sólo hemos de cambiar el enable por **disable**, con esto conseguimos que cuando alguien se quiera conectar a nuestra red necesite saber cual es su nombre (ya modificamos el SSID) y aquí vamos a decirle que lo oculte, es decir que no lo haga público a los equipos ajenos que se encuentren en el radio de acción de nuestro router (aunque es cierto que existen herramientas que no necesitan saber el broadcast del SSID para encontrar la red)

Cifrar la red WPA o WPA2
Lo encontraremos en el apartado **Encryption** de **Wireless Settings**, allí en **Security Mode**, elegimos WPA-PSK o si es posible WPA2, pulsamos sobre Apply y en la nueva pantalla veremos **Pre-shared Key**, escribimos la palabra que hará de clave para proteger la red, recordar de nuevo que ha de ser una clave larga, puede tener hasta 63 caracteres, y debe estar compuesta de letras mayúsculas, minúsculas, números y caracteres especiales. Anotarla para no olvidarla, una vez escrita, pulsamos de nuevo en Apply para guardar los cambios.

Activar el filtrado de direcciones MAC
Primero, por si alguno no sabe exactamente qué es la Mac: (Media Access Control address) es un identificador único e individual en cada tarjeta de red, compuesto de 48 bits en formato hexadecimal, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE, los primeros 24 bits y por el fabricante los últimos 24.

Una vez explicado qué es la Mac, sepamos que filtrando por direcciones Mac, le estamos dando instrucciones al router que sólo permita acceder a los clientes cuyas tarjetas de red tengan las MACs (direcciones físicas) especificadas. Aunque falsificar una MAC no es demasiado difícil para los expertos, al menos ponemos otra medida de protección.

Aquí voy a explicar como conseguir la dirección Mac de nuestras tarjetas, supongamos que tenemos dos PCS, esto que vamos a hacer, debemos hacerlo **primero con uno y luego con otro**, y naturalmente anotar los datos.

Lo mismo que hicimos cuando averiguamos la puerta de enlace predeterminada.

- Pulsamos inicio
- Ejecutar
- Escribimos cmd, y en la pantalla que nos aparece tecleamos **ipconfig /all**
  (tener en cuenta que al final de la g y antes de la barra debéis dejar un espacio)

Os aparecerá una pantalla con, entre otros datos éstos (naturalmente no son los míos)

En estos momentos necesitamos los datos de la dirección física (Mac) pero anotar todos.

Activar el filtrado Mac, lo encontraremos en la sección **Firewall** (por supuesto lo debemos tener enable, activado, es otra medida más) y en **Mac Address Filtering**, allí marcamos la casilla correspondiente y también la de **Access rule for registered Mac Address**, allí marcamos **Allow** y ya sólo nos queda poner las direcciones Mac a las que vamos a autorizar, recordar que debemos poner tantas como equipos tengamos, puesto que ya he dicho que el identificador es único para cada dispositivo.

Desactivar el servidor DHCP
(Dynamic Host Configuration Protocol, que podría traducirse como "Protocolo Dinámico de Configuración de Puestos"). Diseñado por Microsoft, su principal tarea consiste en asignar de manera automática las direcciones IP a los puestos de una red TCP/IP.

Si tenemos esta opción activada en el router, cualquier ordenador que tenga su tarjeta de red configurada en "Obtener una IP automáticamente" y esté dentro del área tendrá acceso a nuestra red.

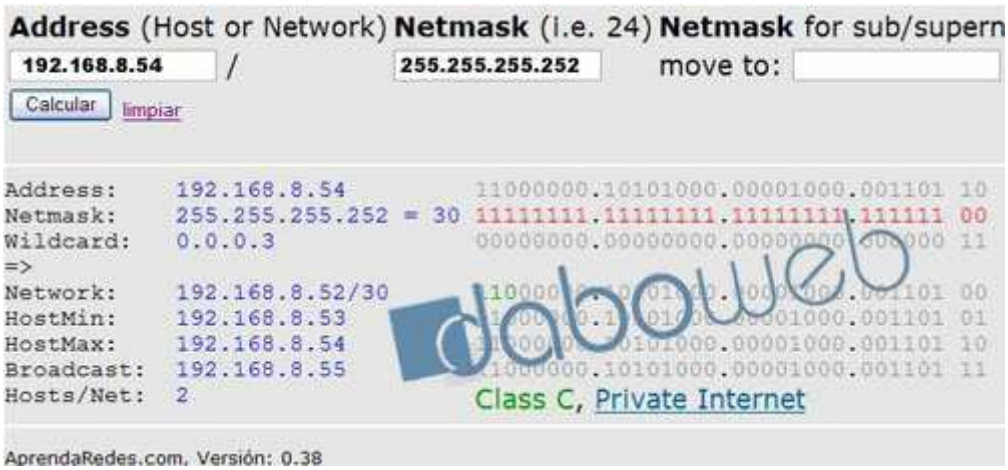
Por tanto vamos a desactivarlo, esto lo haremos en **Lan Settings**, allí lo pondremos en **Off** y le asignaremos las direcciones IPS a los equipos de forma manual.
En IP address pondremos la dirección IP que vimos cuando hicimos ipconfig /all y que nos aparecia como Puerta de enlace predeterminada, que dejamos anotada, normalmente 192.168.1.1, en el apartado **Ip de inicio** (en cada router, aunque son pequeños cambios, algo cambia) pondremos la siguiente es

decir; 192.168.1.2 y en el apartado **end o final**, pondremos algo así como 192.168.1.100, así estamos seguros de poder usar al menos 99 equipos en nuestra lista de rangos IPS. Naturalmente, en los equipos que queramos conectar a Internet deberemos asignarle la IP de forma manual, así configuraremos las IPS de forma consecutiva. Pero para tener mayor seguridad, lo mejor es en el apartado **end o final** dejar acceso a tan sólo los equipos que tengamos, esto lo conseguimos, con el ejemplo de tan sólo 2 pcs conectados, poniendo como ip 192.168.1.3.

Aunque claro, si de verdad queremos asegurarla, lo mejor es poner limitaciones a las IPS mediante Subnettig, que no es otra cosa que modificar la mascara de subred y así restringir el número de dispositivos máximo que pueda convivir en nuestra red.
Aunque esto es más complejo, os explico:
Cuando usamos una dirección del tipo 192.168.1.xx la máscara de subred 255.255.255.0 indica que pertenecen a la misma red lógica todos los dispositivos del rango, es decir desde 192.168.1.1 hasta el 192.168.255. y que en nuestra subred puede tener hasta 255 IPS

Visto todo esto, si nosotros tenemos sólo dos PCS que se puedan conectar a nuestra red, modificando el rango de la máscara de subred, podríamos restringir la conexión a sólo esos dos equipos, por ejemplo si modificamos la máscara de subred y la dejamos en 255.255.255.252, tan sólo tendríamos disponibles las direcciones IPS siguientes:
192.168.1.1 para el router
192.168.1.2 para el primer PC
192.168.1.3 para el segundo
Por tanto, si tenemos los dos PCS conectados, un intruso no podría conectarse en nuestra red, ya que dos direcciones IPS iguales no puede haber en la misma red y libre no le quedaría ninguna.

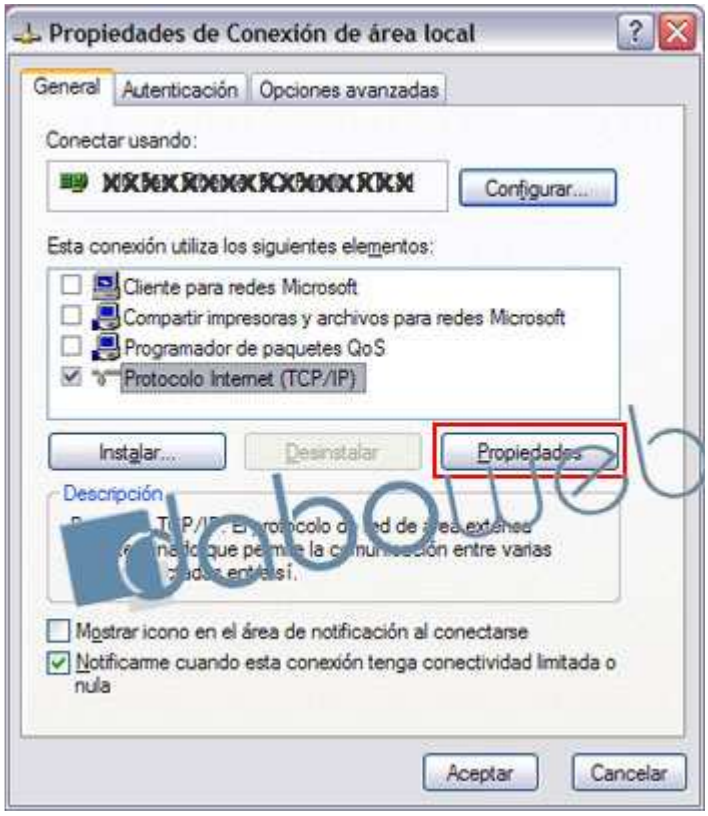
Y ya, si queremos rizar el rizo, y teniendo en cuenta nuestro nivel, lo que podemos hacer es cambiar la dirección ip por una que no sea tan corriente como es la 192.168.1.1, por ejemplo, y contando con restringir, como en el ejemplo anterior a tan sólo 2 equipos el acceso a nuestra red.
Para cambiar la ip, primero debemos comprobar que la ip que pretendemos usar es válida, para ello necesitamos una calculadora de ips (se pueden hacer a mano las comprobaciones, pero para que molestarnos) vamos a esta página, por ejemplo:
http://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi
y ahí, ponemos la dirección ip que pretendamos, y la máscara de subred que como pretendemos que tan sólo puedan conectar 2 equipos, hemos restringido a 255.255.255.252, pulsamos en el botón calcular, e inmediatamente nos dirá si la ip que hemos puesto es válida, también las 2 direcciones ips siguientes a la que le hemos dado y que deberemos poner de forma manual en nuestros 2 equipos, y nos confirmará, lo que nosotros pretendíamos, que sólo 2 equipos se pueden conectar a nuestra red.



Naturalmente, tenemos que tener en cuenta que la seguridad total no existe, por tanto, lo mejor si no la usamos es desactivar la conexión Wifi.

ANEXO:
Para aquel que no sepa como asignar manualmente ips en los equipos, explico brevemente.

Abrimos el panel de control, buscamos y abrimos **Conexiones de red**, en la pantalla que se nos presenta, veremos "Conexión de área local" y en estado, debe aparecer "conectado". Sobre esa opción, **conexión de área local, pulsamos con el botón derecho** del ratón, y elegimos **propiedades**.
Veremos esta pantalla, lo que nos interesa se encuentra en **Protocolo Internet (TCP/IP)**, por tanto lo seleccionamos y pulsamos en **Propiedades**.



Esta nueva ventana aparecerá, dividida como veis en dos partes, en esta explicación la que nos interesa es la de arriba; **Usar la siguiente dirección Ip** la marcamos para que nos deje escribir las direcciones de forma manual.

Puerta de enlace predeterminada: aquí pondremos (siguiendo el ejemplo que antes vimos) 192.168.1.1 (la que vimos como asignada al router).

Dirección Ip: aquí le pondremos la 192.168.1.2, en el primer PC, en el segundo sería 192.168.1.3

Máscara de Subred: como decidimos que limitábamos el rango de PCs que podían conectar en nuestra red a tan sólo 2 (más el router) ponemos 255.255.255.252.
Pulsamos aceptar.

Esto, en los dos PCs, entendiendo, que la puerta de enlace y la máscara de subred han de ser iguales en los dos, la dirección ip, han de ser, en sus últimas cifras, números consecutivos.