

Vida y Obra de un spyware/adware: HotBar

Autor: Lic. Cristian Borghello, Technical & Educational de Eset para
Latinoamérica

Fecha: Sábado 8 de julio del 2006



Presentación

El HotBar ha tenido una alta tasa de propagación en los últimos tiempos, e incluso es común verlo ocupando el ranking de detecciones generado por ThreatSense.Net.

Antes que nada, vale la pena aclarar que un *adware* es un software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario.

Con respecto al *spyware*, software espía, es una aplicación que recopila información sobre una persona u organización sin su conocimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas.

La aplicación en cuestión reúne las dos “propiedades” mencionadas ya que:

- por un lado se instala como una barra de herramientas en nuestro navegador simulando ser una aplicación útil para el usuario y desplegando banners y pantallas publicitarias y;
- por el otro recolecta y envía datos del usuario a través de Internet.

HotBar es una aplicación que agrega icono gráficos en las barras de herramientas de Internet Explorer, Microsoft Outlook y Outlook Express, además de agregar su propia barra de tareas y su propio botón de búsquedas. Esas barras de tareas personalizadas tienen palabras claves predefinidas para alcanzar publicidad luego de instalarse.

HotBar envía información, varios servidores, en función de los hábitos de navegación de los usuarios, los cuales pueden ser explotados para propósitos de mercadotecnia.

También, recoge información acerca de las webs visitadas y la información solicitada en esos sitios, recolecta la IP y las URL que visitadas, y las envía a su servidor para elaborar perfiles estadísticos de los hábitos de los internautas.

Paradójicamente, HotBar ha sido premiado por distintas publicaciones por brindar todas estas características y funcionalidades al usuario.

Instalación

Para comenzar con la pequeña odisea, lo primero que se debe hacer es descargar e instalar esta barra. Cabe preguntarse porqué un usuario haría esto: la respuesta es que este tipo de aplicaciones suelen auto-ofrecer su instalación en los lugares menos imaginados, por lo que es normal que navegando se encuentre con un mensaje de instalación y ante el apuro y desconocimiento, el mismo dé su consentimiento (clic en aceptar).

Aquí es importante remarcar que siempre que se navegue, hay que hacerlo con especial cuidado y protegido con un software que prevenga este tipo de engaños. En este caso, HotBar es detectado por casi cualquier antivirus.

La barra se ha descargado de un conocido y muy visitado portal de noticias, que la ofrece enumerando sus “cientos de ventajas”.



Imagen 1 – “Ventajas” de HotBar

Luego de descargarla, se ofrece instalarla y el usuario creyendo todas las ventajas con las cuales contará, lo hace.



Imagen 2 – Ventana de instalación de HotBar

Igualmente, el sitio de HotBar informa dentro de sus políticas de seguridad que recolectará datos de los usuarios que utilicen su barra de navegación: "Con sólo visitar el sitio de HotBar nosotros recolectamos la siguiente información: Uniform Resource Locator ("URL"), su Internet Protocol ("IP"), la fecha y la hora de cada página visualizada y la información sobre cualquier anuncio que lo trajera al Web site de HotBar".

Más allá de eso, la realidad muestra que prácticamente casi ningún usuario lee este tipo de información. El texto completo, en inglés, puede verse desde el siguiente enlace:

<http://hotbar.com/Legal/hotbar/privacy.htm>

Sería bueno aclarar que los usuarios que tengan instalada la barra de navegación de Hotbar, visitarán el sitio del *adware* cada vez que inicien el navegador, ya que la barra se conecta permanentemente a la web.

Para probar esto, se puede colocar la página por defecto en “about:blank” y al reiniciar el navegador, con una herramienta se puede comprobar que efectivamente se están realizando conexiones al sitio de HotBar. Estas conexiones permanentes ralentizan nuestra navegación y producen una degradación considerable en el sistema.

```

GET /services/hband/ HTTP/1.1
Accept: */*
Accept-Language: es
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; HbTools 4.7.7)
Host: hotbar.com
Connection: keep-alive
Cookie: instcklm%2finstdata%2fiid=f58276638c344a4e9d20feff809f78da7f346834;
Partner=hbtools; Install=; sg=

GET /cscripts/MultiBrand.js HTTP/1.1
Accept: */*
Referer: http://www.hotbar.com/HBservices/autologin/EmailLogin.aspx?Newloc=1
Accept-Language: es
Accept-Encoding: gzip, deflate
If-Modified-Since: Sun, 18 Dec 2005 14:53:10 GMT
If-None-Match: "0cf41c3e23c61:ac3"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; HbTools 4.7.7)
Host: hotbar.com
Connection: keep-alive
Cookie: Install=; srvpers1tid=web06; ASPSESSIONIDCCTABADA=BPPLOFCDOBBFOKAALJOIBJG
    
```

Imagen 3 – Conexiones realizadas al sitio de Hotbar

Una vez que el adware está instalado, se agregan dos nuevas barras en el explorador. En la superior se encuentran varias funcionalidades, mientras que en la inferior se muestra publicidad. Con estos dos nuevos agregados al explorador, se dificulta mucho la navegación, ya que la pantalla de visión se ve sumamente reducida.



Imagen 4 – Barra de Navegación de HotBar

Modificaciones realizadas en el sistema

A continuación, se analizarán las modificaciones que la barra ha realizado en el sistema para dar las “funcionalidades” que ofrece.

En el sistema de archivos, la misma ha descargado e instalado alrededor de 15 Mb que ha sabido diseminar por diferentes sitios de nuestro sistema.

Nombre	Tamaño	Tipo	Fecha de modificación
rb6F.tmp		Carpeta de archivos	26/06/2006 13:45
rb63.tmp		Carpeta de archivos	26/06/2006 13:44
Cml.exe	160 KB	Aplicación	27/03/2006 7:04
dBenderC.dll	288 KB	Extensión de la apli...	27/12/2001 10:57
HbtAds.dll	72 KB	Extensión de la apli...	27/03/2006 7:00
HbtCoreSrv.dll	578 KB	Extensión de la apli...	27/03/2006 7:04
HbtGuard.exe	248 KB	Aplicación	27/03/2006 6:59
HbtHostIE.dll	678 KB	Extensión de la apli...	27/03/2006 7:04
HbtHostOE.dll	52 KB	Extensión de la apli...	27/03/2006 7:03
HbtHostOL.dll	482 KB	Extensión de la apli...	27/03/2006 7:04
HbtInstIE.dll	130 KB	Extensión de la apli...	27/03/2006 7:04
HbtOEAddOn.exe	52 KB	Aplicación	27/03/2006 7:03
HbtTools.mlp	792 KB	Archivo MLP	27/03/2006 7:05
HbtSrv.exe	448 KB	Aplicación	27/03/2006 7:02
HbtToolbar.dll	892 KB	Extensión de la apli...	27/03/2006 7:02
HbtWallpaper.dll	262 KB	Extensión de la apli...	27/03/2006 7:04
HbtWeatherOnTray.exe	248 KB	Aplicación	27/03/2006 7:00

Imagen 5 – Nuevos archivos instalados por HotBar

Aquí es donde se pueden ver todas las numerosas funcionalidades prometidas:

- HotBar propiamente dicha: HbtHostIE.dll, HbtToolbar.dll, HbtCoreSrv.dll, dBenderC.dll, HbtSrv.exe
- Barra del tiempo: HbtWeatherOnTray.exe
- Wallpapers: HbtWallpaper.dll
- Herramientas para Outlook: HbtHostOL.dll, HbtHostOE.dll, HbtOEAddOn.exe
- Archivos de configuración y cookies: nombres aleatorios en diversas ubicaciones.

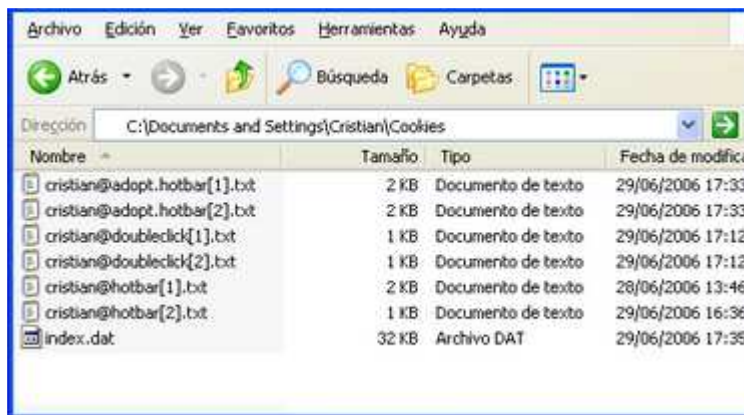


Imagen 6 - Cookies

Las modificaciones realizadas en el registro del sistema le permiten a HotBar ejecutarse cada vez que inicia Windows.



Imagen 7 – Modificaciones en el registro

A continuación, se puede ver que en el administrador de tareas, HotBar también se ha instalado como programa residente. Esto le permite mantener cierto control si el usuario desea borrar los archivos antes mencionados, ya que al permanecer en memoria, el archivo no puede ser eliminado. De todos modos, al menos se permite finalizar el proceso.



Imagen 8 – Administrador de Tareas de Windows

Conclusiones

Como se pudo ver, estas aplicaciones invaden el sistema con objetivos publicitarios y para realizar el rastreo de las acciones llevadas a cabo por el usuario. Esto les permite a estas empresas segmentar el mercado apropiadamente conociendo los hábitos de millones de usuarios alrededor del mundo.

En este caso, se ha tomado como ejemplo una aplicación ampliamente difundida y de relativamente fácil visibilidad y remoción, pero es importante remarcar que otros cientos de estos *malware* podrán dificultar la utilización de la PC.

Como ya se ha mencionado, la mayoría de los antivirus actuales detectan estas aplicaciones, pero debido a que como la misma política de privacidad menciona, estas aplicaciones evolucionan continuamente, es fundamental contar con herramientas con capacidades proactivas que detecte el comportamiento de posibles amenazas de este tipo evitando la instalación de las mismas.