

MyWebSearch: Sonríe, te estamos grabando

Autor: Cristian Borghello, Technical & Educational Manager de ESET para Latinoamérica

Fecha: Martes 16 de Septiembre de 2008

MyWebSearch: Sonríe, te estamos grabando

El creador de la frase *sonríe, te estamos grabando* sin duda tenía una idea muy clara de cómo convencer al público de que esa acción era buena idea y los creadores de **MyWebSearch** han utilizado la misma técnica para instalar su barra en millones de equipos en el mundo.

En realidad, MyWebSearch (o MyWay Speedbar o MyWay Search Assistant o MyWeb SearchBar) no es tan conocida por su nombre como podría ser **FunWebProducts**, cuyo producto más difundido, **Smiley Central**, inunda el navegador con emoticones como los siguientes:



Imagen 1 – Smiley Central

Sin embargo, detrás de estos simpáticos personajes se esconde una historia que no parece ser tan buena idea.

Historia

FunWebProducts es un producto brindado ofrecido por la empresa **IAC Search & Media** que también es propietaria del conocido buscador Ask, que fuera originalmente fundada en 1996 como Ask Jeeves y cambió su denominación en 2005. La información relacionada con la historia de la compañía puede ser consultada en su sitio web:

http://sp.ask.com/en/docs/about/company_overview.shtml

http://sp.ask.com/en/docs/about/fact_sheet.shtml

<http://about.es.ask.com/es/docs/legal/copyright.shtml>

En la nota de Copyright se puede leer el siguiente párrafo:

Avisos de Derechos de Propiedad Intelectual y de Marcas

Todos los contenidos de este Sitio web son titularidad de IAC Search & Media, Inc. y la siguiente reserva de derechos de propiedad intelectual se aplica a todos ellos: Copyright (c) 2007 IAC Search & Media, Inc. Todos los derechos reservados.

Puede verse fácilmente que en esa historia no se menciona nada de la relación de Ask con FunWebProducts y con IAC Search & Media, si bien al pie de todos los sitios web relacionados aparece “© 2008 IAC Search & Media. Todos los derechos reservados” y también aparece al pie de la página como puede verse en la siguiente imagen:

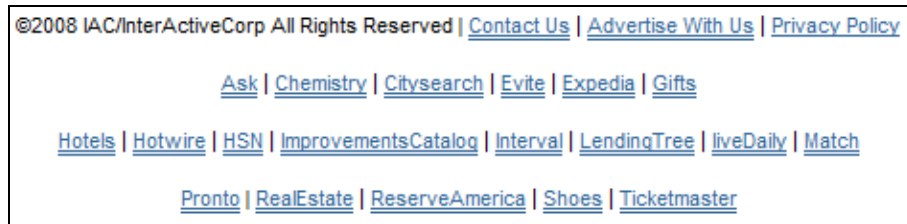


Imagen 2 – Copyright de IAC Search & Media

Además, si se consulta la información de Ask, FunWebProducts, Smiley Central y MyWebSearch, puede corroborarse fácilmente esta relación:

<p>WHOIS - ask.com</p> <p>Generated by www.DNSstuff.com</p> <p>Registrar: CSC CORPORATE DOMAINS, INC. Status: clientTransferProhibited Dates: Created 20-oct-1998 Updated 21-ma DNS Servers: NAME1.ASKJEEVES.COM NAME5.ASK.COM</p>	<p>WHOIS - funwebproducts.com</p> <p>Generated by www.DNSstuff.com</p> <p>Registrar: CSC CORPORATE DOMAINS, INC. Status: ok Dates: Created 18-jun-2003 Updated DNS Servers: NAME5.ASK.COM NAME6.ASK.COM</p>
<p>WHOIS - smileycentral.com</p> <p>Generated by www.DNSstuff.com</p> <p>Registrar: CSC CORPORATE DOMAINS, INC. Status: clientTransferProhibited Dates: Created 30-apr-2003 Updated DNS Servers: NAME5.ASK.COM NAME6.ASK.COM</p>	<p>WHOIS - mywebsearch.com</p> <p>Generated by www.DNSstuff.com</p> <p>Registrar: CSC CORPORATE DOMAINS, INC. Status: clientTransferProhibited Dates: Created 10-dec-2001 Updated DNS Servers: NAME5.ASK.COM NAME6.ASK.COM</p>

Imagen 3 – Whois de los productos de Ask

Es por este motivo que Ask es el buscador que queda como predeterminado al instalar cualquiera de las barras que se mencionan a continuación.

Productos y servicios brindados

FunWebProducts es un conjunto de herramientas brindadas por la empresa IAC Search & Media en forma gratuita, entre las que pueden hallarse las siguientes:

- **My Web Search:** barra de herramientas que ayuda a realizar búsquedas en Internet utilizando varios motores.
- **MyWay:** página de inicio la cual se puede utilizar para acceder directamente a cualquiera de los otros servicios.
- **Smiley Central:** permite insertar emoticones y otros gráficos en los chat de los mensajeros instantáneos y en el correo electrónico.
- **Cursor Mania:** permite cambiar el aspecto del cursor del mouse.
- **Icons Fun Buddy:** permite agregar iconos a los clientes de mensajería instantánea.
- **History Swatter:** permite eliminar las cookies, el historial de navegación, la caché y otros archivos almacenados por el explorador.
- **My Fun Cards:** proporciona tarjetas electrónicas personalizables que se pueden enviar a otro usuario a través del correo electrónico.
- **My Info:** proporciona acceso al pronóstico del tiempo, a los valores de bolsa, resultados deportivos, noticias de actualidad, horóscopo, etc.
- **My Mail Notify:** permite utilizar personajes animados para avisar cuando se reciben mensajes de correo nuevos.
- **My Mail Sign:** permite crear diseños de firmas para los mensajes de correo electrónico.
- **My Mail Stamp:** permite insertar diseños de sellos postales digitales en los mensajes de correo electrónico.
- **Popular Screensavers:** proporciona fotos e imágenes que pueden utilizarse como protector de pantalla o papel tapiz.
- **Smotos:** permite publicar, compartir y descargar imágenes.

- **Otros servicios son:** Search Assistant, PopSwatter, iWon, Zwinky, Web Fetti, Smiley Arcade y decenas más:



Imagen 4 – Servicios de Fun Web Products

Cada una de estas herramientas tiene su propio sitio web que promociona sus supuestas ventajas de diferentes maneras. La insistencia en la gratuidad de las aplicaciones ("It's Free", "Download Free", etc.) tiene el objetivo de tentar al usuario a descargarlas e instalarlas, lo que posteriormente le causará inconvenientes y perjudicará el normal funcionamiento de su sistema.



Imagen 5 – Productos gratuitos

Instalación

La forma más común de encontrar e instalar algunas de estas herramientas es a través de adware [1], banners, pop-pus o publicidad online que las ofrece (protectores de pantalla, smiley, cursores, etc.) y que redirigen al usuario al sitio web de la aplicación que corresponda (cualquiera de ellas)

Una vez descargada e instalada la aplicación, se puede ver la barra elegida sobre el navegador, el cliente de correo o el mensajero y posteriormente se ofrecerá descargar y establecer MyWebSearch como barra de búsqueda predeterminada.

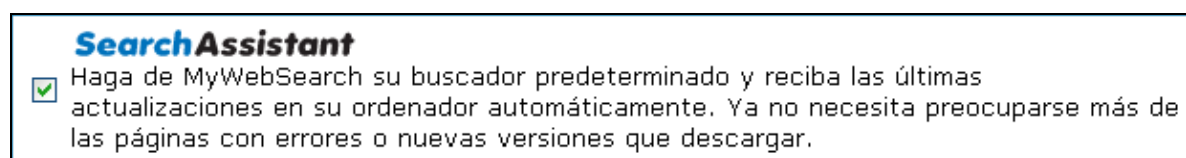


Imagen 6 – MyWebSearch como barra de búsqueda por defecto

Aquí se nota el primer comportamiento extraño de esta aplicación, ya que cualquiera de los productos que se instalen, también instalarán por defecto la barra de búsqueda cambiando el comportamiento normal del sistema anfitrión y de sus aplicaciones.

Como se puede ver a continuación, luego de la instalación de Smiley Central en este caso, se han agregado barras, botones y menús de otras herramientas, ya sea en el navegador como en el cliente de correo:

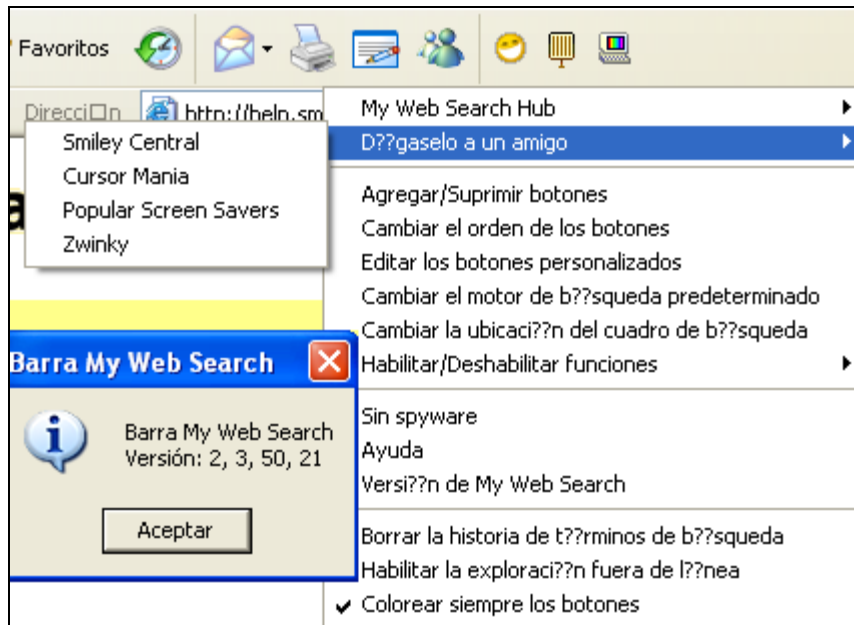


Imagen 7 – Barras agregadas por MyWebSearch al navegador

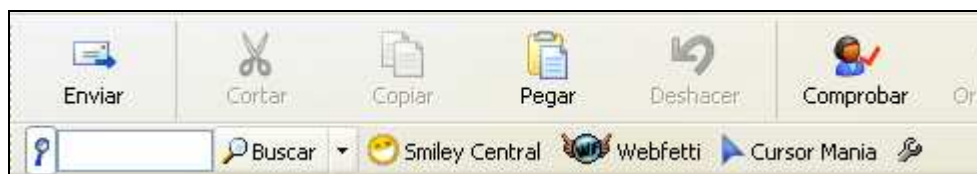


Imagen 8 - Barras agregadas por MyWebSearch al cliente de correo

NOTA: para el desarrollo del presente, los productos han sido probados e instalados en Microsoft Internet Explorer y Outlook Express (6 o superior) debido a que la licencia de MyWebSearch indica que éstos son el navegador y el cliente de correo adecuados.

Una vez instalada MyWebSearch, la barra de búsqueda propiamente dicha dirige al usuario a su sitio web y permite que el mismo realice sus búsquedas a través de diversos motores como Ask, Google, Yahoo! y LookSmart, enviando los términos buscados, la configuración de los productos y la dirección IP del usuario a sus servidores centrales. Esta información puede ser entregada a terceros si la misma es

requerida, como puede leerse en su EULA (End User License Agreement - en español, Contrato de Licencia de Usuario Final):

<http://helpint.mywebsearch.com/intlinfo/eula/eula.jhtml#privacy>

Según esta licencia, el objetivo de la recolección de esta información es agregativo y estadístico para monetizar y realizar publicidad sobre las búsquedas más comunes. Es decir que la información recolectada tiene el objetivo de realizar estadísticas para elaborar perfiles de los hábitos de los internautas.

Otra forma común de instalar este tipo de aplicaciones es a través de software del tipo **Bundle**, programas que forman parte o acompañan a otro software y se instalan (generalmente con la autorización del usuario) luego de instalarse el primero. Este método consiste en mostrar una pantalla al usuario, y en la misma presentar una casilla de selección (generalmente ya marcada) donde se acepta la instalación. Si el usuario no lee o no presta atención al contenido de la pantalla, el software se instalará.

La casilla marcada por defecto puede verse en la imagen 6 y en la siguiente, al momento de instalar una conocida aplicación que tiene a MyWebSearch como Bundle:



Imagen 9 – Instalación Bundle

En este caso se utiliza la falta de atención del usuario en su contra, para lograr la instalación de la aplicación, con la aceptación de términos y condiciones incluidos, haciendo al usuario responsable de los mismos. Las instalaciones del tipo Bundle se utilizan a menudo en aplicaciones gratuitas para lograr ganancias que de otra forma no serían obtenidas.

Aplicación potencialmente indeseada

Luego de lo descrito se llega a la conclusión de que el software creado por FunWebProducts contiene **aplicaciones potencialmente indeseadas**, ya que si bien los comportamientos de las mismas no suelen ser dañinos, son perjudiciales para el rendimiento del sistema por los siguientes motivos:

- Se modifica la página de inicio del usuario.
- Se cambia el motor de búsqueda del usuario.
- Al momento de instalar una aplicación, se instalan otras no solicitadas.
- Se envía información a los servidores centrales de la aplicación.
- Se consumen recursos del sistema operativo y de las aplicaciones, de forma tal que se destina tiempo de procesamiento a aplicaciones no deseadas.
- Por el motivo anterior, el navegador, el cliente de correo y otras herramientas se ralentizan por las aplicaciones extras instaladas.
- Toda la información procesada por las barras es actualizada constantemente desde un servidor central, lo que incrementa el tráfico en la red. El usuario experimentará una caída notable del rendimiento de su conexión a Internet.
- Cada cierto tiempo, pueden ofrecerse nuevas aplicaciones para instalar en pop-pus que aparecen en el navegador.
- La desinstalación de las aplicaciones puede ser confusa y pueden experimentarse fallos debido a programas "faltantes".
- Los resultados de las búsquedas pueden verse alterados por mensajes de publicidad de empresas patrocinadoras de las barras instaladas.
- Se instalan BHO¹ en el navegador que modifican su comportamiento.
- Se modifican las páginas de error normales entregadas por el navegador y por lo general se publicitan productos y servicios en las mismas.
- Se modifica el comportamiento de la barra de direcciones del navegador y, si el usuario ingresa una dirección no válida, puede ser dirigido a sitios de promociones y ofertas.

¹ **Browser Helper Object (Objeto de ayuda del navegador)**: componente que es ejecutado automáticamente por el navegador para extender alguna de sus funcionalidades.

- La navegación se puede ver alterada por la aparición de publicidad, adware o ventanas no solicitadas.
- Las aplicaciones extras instaladas, al ser software, pueden tener vulnerabilidades que permitan infectar o vulnerar el sistema huésped.

La instalación de este tipo de aplicaciones es muy común actualmente debido a las supuestas ventajas que ofrecen a los usuarios pero lamentablemente se vuelven un dolor de cabeza debido a la gran cantidad de acciones no solicitadas que realizan, justificando sus acciones o bajo la excusa de que el usuario es responsable de las mismas ya que aceptó instalarlas.

Además conviene recordar que estas aplicaciones suelen consumir recursos del sistema y ancho de banda por conexiones innecesarias, ralentizando el mismo y ocasionando un mal funcionamiento del sistema operativo y las aplicaciones instaladas por el usuario.

Por estos motivos ESET NOD32 detecta este tipo de software como **Aplicaciones potencialmente indeseables** y le informará al usuario cada vez que el mismo intente descargarlas o instalarlas:

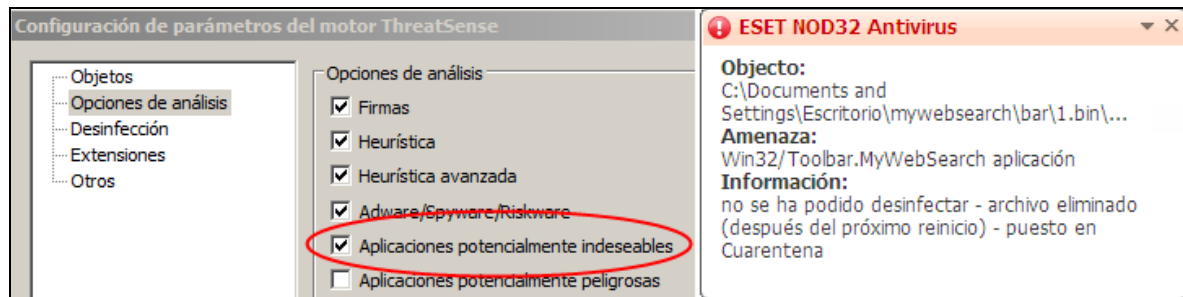


Imagen 10 – Detección de Aplicaciones potencialmente indeseables por ESET NOD32

Vulnerabilidades extras

Como se mencionó anteriormente, este tipo de software puede incluir vulnerabilidades como cualquier otro e incluso esta posibilidad es mayor debido a que el usuario desconoce que debe actualizar estas aplicaciones.

También existe la posibilidad de que sus desarrolladores desconozcan estas vulnerabilidades y por ende nunca solucionen sus problemas.

Esta situación da pie a que las vulnerabilidades puedan ser explotadas por personas maliciosas y que las mismas puedan lograr el control del equipo afectado, robando información confidencial del usuario, infectándolo con malware, redirigiéndolo a sitios de phishing, etc.

A continuación se incluyen dos ejemplos. Con el primero de ellos se puede averiguar si alguna de las aplicaciones mencionadas ha sido instalada en el cliente.

Para ello se ejecuta un simple *script* que informará efectivamente que una aplicación de FunWebProducts se encuentra instalada y ha modificado el nombre del agente de navegación por defecto:



Imagen 11 – Nombre del agente de navegación modificado por FunWebProducts

Ahora que el supuesto atacante conoce que este producto está instalado puede explotar una vulnerabilidad [2] en el mismo y, por ejemplo, obtener las cookies del usuario para luego utilizarlas en otro tipo de ataques que excederían el presente:

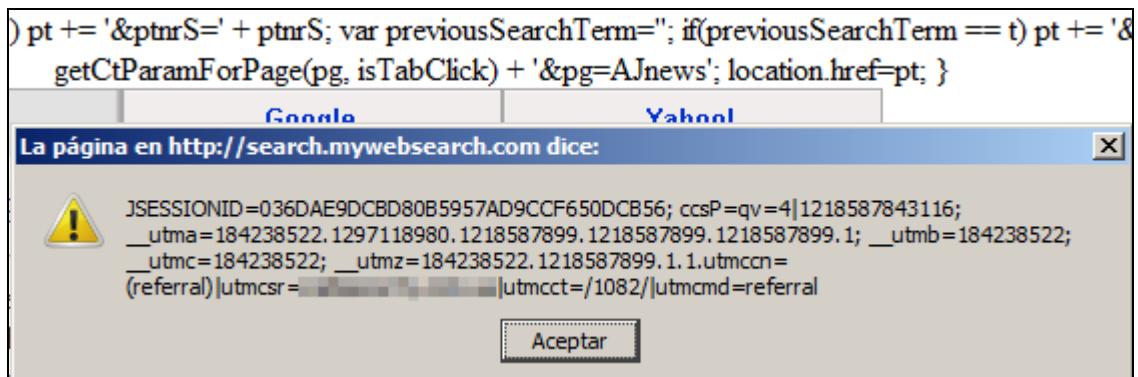


Imagen 12 – Visualización de Cookies a través de vulnerabilidad en MyWebSearch

Es decir que con el simple hecho de instalar la aplicación se abre una puerta en el sistema para que cualquier persona inescrupulosa pueda aprovecharla en contra del usuario.

Conclusiones

Es muy normal encontrar el tipo de aplicaciones descritas instaladas en los equipos de los usuarios debido a la gran cantidad de servicios que ofrecen, pero también es importante notar que su instalación tiene un precio, que si bien no es económico, está relacionado con el valor que el usuario da a su información, su privacidad y la buena salud de su sistema.

Se debe prestar especial atención para evitar la instalación de aplicaciones del tipo Bundle y para ello es recomendable que las mismas sean detectadas por soluciones antivirus que eviten su descarga y/o instalación.

El usuario es el principal responsable de controlar y evitar la instalación de las aplicaciones potencialmente indeseables disponibles en Internet, desconfiando de las bondades que las mismas ofrecen.

[1] Vida y obra de un adware/spyware: Hotbar

<http://www.eset-la.com/threat-center/1603-vida-obra-spyware-adware-hotbar>

[2] Vulnerabilities at search.mywebsearch.com

<http://websecurity.com.ua/1082/>