

## Seguridad y navegadores de Internet: Firefox versus Internet Explorer

### Introducción

Internet se está convirtiendo cada vez más en un lugar peligroso, debido, en gran medida, a los riesgos de seguridad inherentes que presentan los virus y programas espía.

Además, las aplicaciones que acceden a Internet, como parte de su funcionamiento habitual, pueden contener errores en sus códigos que permitan a los piratas lanzar ataques contra el ordenador en el que se están ejecutando esas aplicaciones. La seguridad e integridad de los bienes digitales se comprometen aún más debido a la creciente amenaza de los piratas cibernéticos que diseñan e implementan estafas a gran escala, como por ejemplo la falsificación de direcciones IP y el robo de identidad.

En vista de esto, está claro que los usuarios necesitan un navegador de Internet confiable y seguro, entre ellos e Internet, que esté libre de estos problemas y no permita que algún tipo de contenido perjudicial invada su ordenador.

La industria de navegadores de Internet sigue siendo dominada por Internet Explorer que está incorporado en Windows, con un 85% de participación en el mercado, pero recientemente apareció una nueva variedad de navegadores gratuitos, más funcionales y resistentes, de los cuales los más populares son Mozilla/Firefox y Opera. Todos han recibido actualizaciones de seguridad importantes para protegerse contra recientes amenazas y cuidar a los usuarios en línea.

Internet Explorer se encuentra en su versión 6.0, básicamente el mismo producto que estaba incluido con Windows XP en 2001. Hace dieciocho meses, el lanzamiento de Windows XP Service Pack 2 incrementó la seguridad de Internet Explorer de manera significativa, pero sin embargo, no eliminó muchas de las lagunas explotadas por los códigos de programas dañinos. En la actualidad, Firefox se encuentra en su versión 1.5, pero su historia de desarrollo diferente (ver próxima sección) significa que puede considerarse a un nivel similar de madurez que Internet Explorer.

Actualmente, Microsoft está preparando su navegador de próxima generación, Internet Explorer 7.0, el cual se estima que se presentará durante la primera mitad de 2006.

La empresa declaró que tiene la intención de desarrollar un navegador más potente y seguro, para de ese modo ayudar en la protección de los usuarios contra los numerosos problemas que han perseguido a las aplicaciones a lo largo de los años.

Nosotros, junto con los usuarios de Internet en todo el mundo, esperamos los resultados finales con gran interés. Mientras tanto, decidimos llevar a cabo nuestra propia evaluación de seguridad de Internet Explorer 7 (beta) y su rival más cercano, Firefox 1.5

### Historia y reseña

#### Internet Explorer

Es un navegador de Internet, con tecnología propietaria, con interfaz gráfica, desarrollado por Microsoft.

En 1995, la empresa obtuvo la licencia para la versión comercial de Internet Explorer 3.0 de Spyglass Mosaic e integró el programa en la edición de Windows 95 OSR1.

Más adelante, incluyó Internet Explorer 4 como el navegador predeterminado en Windows 98, una jugada que continúa generando mucha polémica en relación a la posible existencia de monopolio.

#### Firefox

Es un navegador de código abierto, desarrollado por Mozilla Foundation, y cualquier persona que sea lo suficientemente experta puede colaborar en el desarrollo y mejora del código del programa.

Mozilla es conocida por su enfoque estricto hacia la seguridad, y la promesa de una recompensa de varios cientos de dólares para cualquier vulnerabilidad significativa que se encuentre en el producto.

## Incidentes relacionados con la seguridad y respuesta a las amenazas

Si bien ningún navegador es perfecto, surgieron fallas de seguridad importantes bastante más a menudo con Internet Explorer que con Firefox. Para ser justos, Firefox tiene menos del 10% de participación en el mercado y, por consiguiente, es un objetivo menos atractivo que Internet Explorer; probablemente es por eso también que los investigadores de seguridad concentran su atención en las vulnerabilidades del navegador de Microsoft y no en las de Firefox. Se ha argumentado también que si la participación en el mercado fuera a la inversa, comenzarían a aparecer problemas en Firefox de forma más frecuente, como sucedió recientemente con Internet Explorer.

La arquitectura de código abierto de Firefox contribuye a la seguridad general del navegador; una comunidad de expertos programadores puede detectar problemas más rápidamente y corregirlos antes de que esté disponible una nueva versión para uso general. Se ha indicado que el tiempo de respuesta a las amenazas para Firefox promedia una semana, mientras que puede llevar meses para que los ingenieros de Microsoft arreglen problemas críticos informados por analistas de seguridad, una situación inaceptable para usuarios que siguen siendo innecesariamente vulnerables a los ataques (de piratas) durante ese tiempo.

Desde el punto de vista de respuesta ante una amenaza, Firefox es claramente el ganador.

## Rutas posibles para los ataques

### Protección contra falsificación de direcciones de Internet y técnicas de *Phishing*

La nueva protección contra el fraude financiero y el robo de identidad, ha sido incorporado en el nuevo Internet Explorer.

Ahora se cuenta con un denominado **filtro contra falsificaciones**, que aparece en el menú de opciones de Internet, y que tiene la intención de proteger a los usuarios contra la divulgación de información privada, a terceros no autorizados, sin el correspondiente consentimiento.

Esta opción funciona de la siguiente manera:

Si un usuario visita un sitio falso, que parece exactamente igual que el original, por lo general después de pulsar sobre un enlace en un correo electrónico fraudulento, el navegador detecta un intento de falsificación de dirección y compara el sitio con una lista de sitios conocidos de falsificación de direcciones.

Si el filtro detecta que el sitio es culpable de falsificar la dirección, bloquea el acceso al mismo e informa al usuario del peligro de dejar su información personal en sitios como ese.

La base de datos de sitios conocidos con direcciones falsificadas, se actualiza de forma regular y los usuarios tienen la opción de informar una instancia sospechosa de falsificación a Microsoft, para una evaluación.

Tenemos el agrado de informar que, incluso en la versión beta, el filtro parece funcionar bastante bien, identificando de manera correcta la mitad de los sitios de prueba que visitamos conocidos como sitios de falsificación de direcciones de Internet.

En Firefox, la protección contra *Phishing* (falsificación de direcciones) se presenta a través de extensiones de terceros, como por ejemplo **Google Safe Browsing** (navegación segura de Google) y que actualmente se encuentra en su versión beta para usuarios residentes en Estados Unidos únicamente: <http://www.google.com/tools/firefox/safebrowsing/index.html> y esto puede incluirse en el menú de extensiones del navegador.

Como protección adicional contra falsificación de direcciones accidentales, los creadores de Internet Explorer indicaron que planean hacer que su producto muestre la dirección de Internet de cada sitio visitado.

Con Internet Explorer 6, esta funcionalidad no estaba disponible y aparecían muchos cuadros de diálogo, sin mostrar una dirección en una barra de direcciones que no existía.

Desafortunadamente, en ninguno de los dos navegadores pudimos lograr un índice de más del cincuenta por ciento de direcciones mostradas.

Confiamos en que este porcentaje se incrementará a medida que se acerque el lanzamiento de Internet Explorer 7 y que Mozilla continúe trabajando en la mejora de dicha funcionalidad en esta área.

### Restricción de contenido ejecutable de Internet

En la versión actual de Internet Explorer, los sitios sospechosos de Internet han tenido la libertad de instalar casi cualquier programa que desearan en los ordenadores de los visitantes.

Si bien Windows XP Service Pack 2 redujo de manera significativa esta posibilidad, todavía los usuarios no experimentados pueden instalar fácilmente muchos complementos y barras de herramientas innecesarios.

Internet Explorer 7 debería brindar más protección a los usuarios inexpertos, dado que ofrecerá ejecutarse en modo protegido y, por consiguiente, restringirá el acceso a los archivos *hosts* y configuraciones del sistema operativo, lo cual evitará que estos elementos críticos del ordenador estén disponibles para programas espía.

La configuración predeterminada para Firefox 1.5 es desactivar la instalación de extensiones y complementos y el usuario deberá modificar la configuración manualmente para poder agregar extensiones al navegador.

Siempre existirá un equilibrio entre seguridad y funcionalidad, pero los expertos en seguridad siempre indicaron que permitir que los sitios de Internet lancen código ejecutable sin restricciones dentro del navegador, crea un potencial ilimitado para la explotación.

Internet Explorer 7 ofrecerá una mayor flexibilidad en la configuración del código externo que podrá ejecutarse dentro del navegador y el impacto que el mismo tendrá sobre el sistema operativo.

#### **Restricciones para código ActiveX**

Más allá de la mejora en los gráficos de las páginas de Internet, en la mayoría de los casos, **ActiveX** es mucho más perjudicial que beneficioso.

Muchos sitios que ofrecen programas espía y ventanas con publicidad, utilizan tecnología de guiones **ActiveX**, y estos pueden ejecutarse en el entorno de Windows sin restricciones y con privilegios de administrador (*Root*).

Firefox 1.5 no soporta la tecnología **ActiveX** propietaria de Microsoft y, por lo tanto, el navegador de Firefox es más resistente contra infección de programas espía.

En Internet Explorer 6, incluso con SP 2, **ActiveX** puede ejecutarse de manera predeterminada, lo que automáticamente deja a los usuarios de Internet Explorer más indefensos contra la amenaza de programas espía.

En la próxima versión de Internet Explorer 7, todavía no se sabe si Microsoft continuará con este enfoque, pero las primeras indicaciones apuntan a que será así.

Esto no sería del todo afortunado, dado que el enfoque actual es una clara vulnerabilidad de la seguridad.

Por supuesto, los usuarios de Internet Explorer pueden desactivar manualmente los guiones ActiveX de un sitio en particular, y permitir que ActiveX se inicie de manera automática en el resto de los sitios visitados. O, a la inversa, pueden desactivar los guiones ActiveX en la mayoría de los sitios visitados y permitir que se ejecuten en un sitio en particular.

Todo esto puede configurarse en la pestaña seguridad del menú Opciones de Internet Explorer.

Sin embargo, es poco realista esperar que los nuevos usuarios de Internet, que son quienes necesitan la mayor protección, puedan hacer esto.

#### **Componentes Java, JavaScript y Visual Basic**

Java y JavaScript pueden ser activados y desactivados por ambos navegadores.

Firefox permite, a los usuarios, especificar permisos para acciones específicas realizadas por estos guiones. Internet Explorer 6 permite, a los usuarios, crear un grupo de sitios de confianza a los que no se aplicarán limitaciones globales sobre estos guiones.

En Internet Explorer 7 se agregará más flexibilidad, lo que llevará a los usuarios a una visualización más personalizada de páginas de Internet pertenecientes a un sitio en particular.

Aparentemente Firefox también planea introducir parámetros más flexibles.

#### **Administrador interno de descargas**

El administrador de descargas de Internet Explorer 7 será rediseñado y presentará una opción para pausar y reanudar las descargas, una característica que no está disponible en la versión actual.

Se podrán definir acciones específicas después de completar la descarga y, los usuarios, podrán verificar el archivo recién descargado con su programa antivirus, antes de ejecutarlo.

Este enfoque ya se encuentra en funcionamiento en Firefox, por lo que parece que Microsoft se está poniendo a tono en este caso.

#### **Encriptación de datos en sitios protegidos**

Cuando se envía información confidencial, como por ejemplo, detalles de operaciones a un banco o institución financiera, viaja de forma encriptada a través de una conexión HTTP segura (SHTTP).

La información es encriptada por el navegador y desencriptada en el destino.

La nueva versión de Internet Explorer utiliza algoritmos de encriptación más potentes para transferir sus datos de manera confiable, sin el riesgo de ser interceptados y descifrados por alguna persona durante el tránsito.

Se colocará un icono de un candado, que indica que el usuario se encuentra en un sitio seguro, en un lugar más obvio que el actual, y se brindará más información detallada para ayudar a los visitantes a verificar la autenticidad de tales sitios.

Firefox tiene actualmente una visualización más organizada de los certificados de seguridad para los usuarios, por lo que es claro que Microsoft todavía puede implementar una mejora.

## Actualización

Ambos navegadores se actualizan de forma automática cuando se encuentra disponible nuevo código base. Firefox ya cuenta con un mecanismo de actualización en funcionamiento, y para Internet Explorer 7, se espera que las actualizaciones aparezcan a través de la tecnología de actualización Windows Update.

## Mejoras en la privacidad

Internet Explorer 7 tendrá la capacidad de que los usuarios establezcan de manera flexible qué datos privados se guardarán y cuáles podrán ser aplicados a diferentes sitios.

Los usuarios podrán eliminar fácilmente el historial de navegación y otros detalles privados tales como:

- Contraseñas
- *Cookies*
- Detalles enviados en formularios de Internet
- Historial de descargas
- Archivos temporarios

En Internet Explorer 6, estos archivos eran almacenados en diferentes lugares y los usuarios se han quejado que no existe una forma clara de eliminar esta información.

Firefox 1.5 ya brinda esta funcionalidad.

## Conclusión

Internet Explorer 7 promete muchas mejoras interesantes en seguridad y privacidad, que ayudarán a los usuarios a estar más protegidos.

Con la versión final los usuarios recibirán un buen navegador potente que, si se cumplen las promesas de Microsoft, será un buen competidor en el área de seguridad.

Como hemos visto, Firefox 1.5 ya es un modelo de conducta y sería interesante ver lo que nos depara este competidor talentoso.