PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 9 | ENERO 2011 | ISSN EN TRÁMITE | REVISTA BIMESTRAL

Editorial

El navegador web es hoy por hoy una de las aplicaciones más populares en el mundo, a través de éste podemos conectarnos a una gran cantidad de información, se ha convertido en herramienta indispensable para la realización de muchas tareas, sean escolares, de oficina, de negocios o gubernamentales.

El uso extendido del explorador para todo tipo de operaciones ha hecho de éste un blanco recurrente para los criminales cibernéticos, al ver en él muchas posibilidades de tomar ventaja de errores o vulnerabilidades no corregidas.

Es importante comprender que el navegador, sea cual sea, no tiene garantizada una seguridad informática al cien por ciento, por ello una vez más la información precisa y la prevención son las mejores aliadas para superar estas dificultades.

Por ello, en esta ocasión, la revista .*Seguridad* te ofrece recursos informativos para que consideres aspectos importantes sobre tu navegador y la rutina sugerida al estar conectado, con estos consejos podrás reducir los riesgos y aumentar la eficiencia al consultar o realizar tus labores.

¡Bienvenido! Esperamos esta edición sea de tu agrado.

Galvy Ilvey Cruz Valencia
Subdirección de Seguridad de la Información

Angie Aguilar Domínguez

¿Qué es un navegador web?

Es una aplicación que se ejecuta en la computadora, nos sirve para ver la información contenida en una o varias páginas web. Para poder consultarla, primero interpreta y luego la muestra en pantalla. Esto nos permite ver documentos con imágenes, audio y otros recursos incrustados. El navegador web también es conocido como explorador.

Un navegador es necesario, pues el formato de los documentos que visitamos en la web emplean distintos elementos (como un enlace a otra página, por ejemplo), y su realización se lleva a cabo utilizando algún lenguaje especializado que posteriormente el navegador descifrará. Así como se emplea alguna aplicación como *Microsoft Word* para visualizar archivos *.doc*, de la misma manera se emplea un navegador para poder ver archivos *.html* y *.php*, entre otras extensiones usadas en la red.

La mayoría de los navegadores tienes características similares, como lo son: la navegación por pestañas (se abre una nueva página en la misma ventana, en lugar de abrir una nueva ventana), la posibilidad de bloquear las ventanas emergentes (como algunos anuncios o juegos), soporte para motores de búsqueda (como *yahoo!* o *google*), también poseen un gestor de descargas (facilitan la descarga de archivos de una página web), uso de marcadores (guía de páginas favoritas), corrector ortográfico, y algunos atajos del teclado (por ejemplo, tecla *ctrl* + *t* para abrir una nueva pestaña).

Así mismo, para mantener la privacidad, algunos de ellos permiten un manejo sencillo de borrado del historial de las páginas que han sido visitadas, así como algunos datos que son recordados (como las cookies y el caché).

A algunos navegadores web se les pueden añadir funcionalidades extra, conocidas como extensiones, ya que no se encuentran dentro de la funcionalidad básica.

¿Qué hace diferente a un navegador web de otro?

Una de las diferencias más notables entre los diferentes navegadores web existentes consiste en cómo nos muestra la página visitada. Ocurre a menudo que, si visitamos una página con un navegador X y a la vez, con un navegador Y; notamos que en esencia se muestra la misma información, sin embargo existen diferencias entre uno y otro: como el color o alguna funcionalidad deshabilitada. Esto se debe al *motor de renderizado* de cada uno de ellos.

Un motor de renderizado hace referencia a un software que toma tanto contenido, como información del formato de presentación de la página y luego nos la presenta como un conjunto de ambos.

De la misma manera, otra diferencia importante entre un navegador y otro es *el motor de javaScript* que emplean. Este motor permite la ejecución de código *javaScript*, el cual busca facilitar la interacción entre las personas y la página web que se encuentran visitando.

Uno de los más populares es el del navegador *Mozilla Firefox,* cuyo nombre es *Gecko*. Para el caso de los navegadores web *Google Chrome* y *Safari*, el motor de renderizado se llama *WebKit*. El motor de renderizado de *Internet Explorer* se llama *Trident* y para el navegador *Opera* el motor se llama *Presto*.

A continuación se exponen los logotipos de los navegadores mencionados:

Internet Explorer

Mozilla Firefox

Safari

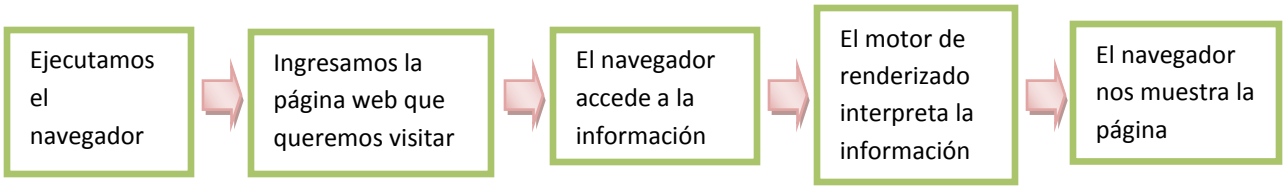
Opera

Chrome

Todos los navegadores web tienen motor de renderizado y cada uno de ellos posee características que lo hacen diferente de los demás. Como nota adicional, algunos navegadores no desarrollan su propio motor de renderizado, por lo que emplean otro ya existente.

Tal es el caso del navegador web *Flock* (navegador web orientado a las redes sociales), el cual hasta hace poco tiempo empleaba como motor de renderizado a *Gecko*, pero actualmente emplea *WebKit*.

El funcionamiento general de un navegador web, cuando nos muestra una página web se puede ver en el siguiente diagrama:



Gecko es un proyecto de software libre (cualquier persona interesada, puede ver cómo está implementado y además si lo desea, puede modificarlo) que inició con *Netscape* (un navegador web empleado desde los comienzos de Internet), cada modificación o mejora es realizada por la Fundación Mozilla.[1]

Ofrece soporte para diferentes estándares web que se manejan para llevar a cabo la implementación de las páginas que visitamos; de la misma manera, es multiplataforma, lo que quiere decir que funciona en distintos sistemas operativos, como *Windows*, *Linux* o *MacOS*, por ejemplo.

Otra de sus características es que se encuentra implementado de forma modular, lo que quiere decir que se tienen bloques de funciones bien definidas; de esta manera, llevar a cabo una nueva implementación, no involucra modificar ninguno de los bloques de funciones existentes. De la misma manera, permite la implementación de extensiones complementarias al navegador.

Webkit

El motor de renderizado, *WebKit,* posee las siguientes características: está desarrollado bajo la filosofía del software libre, posee una buena compatibilidad con los estándares en los que se encuentran implementadas la mayoría de las páginas web, también es multiplataforma.

Debido a estas características, es considerado una buena opción para ser empleado por navegadores como *Safari* o *Chrome* y otros menos conocidos, pero también empleados.

Este motor de renderizado, también es empleado en los teléfonos conocidos como *smartphone* (teléfono inteligente que provee funcionalidades adicionales como un cliente de correo electrónico) que cuentan con el sistema operativo *Android,* ya que proveen conectividad a Internet mediante alguna variante de un navegador web.

Trident

Para el caso de *Trident*, es el motor de renderizado empleado por *Internet Explorer*, es el motor menos compatible con los estándares para el desarrollo de páginas web[2]. Por ello, muchas páginas no han sido diseñadas para ser compatibles con los estándares existentes, sino para ser compatibles con el motor empleado por *Internet Explorer*. Sin embargo, es uno de los motores más empleados ya que un gran número de usuarios emplea este navegador para visitar páginas web.

[1] Wikipedia. http://es.wikipedia.org/wiki/Gecko_(motor_de_renderizado)
[2] W3C. http://www.w3schools.com/browsers/browsers_stats.asp

Presto

Presto es el motor empleado por el navegador web *Opera*, el cual posee buen soporte para los diferentes estándares empleados por las páginas web. Es desarrollado por Opera Software y es multiplataforma.

Seguridad

Es importante tener en cuenta que todos los navegadores poseen huecos de seguridad, y éstos pueden poner en riesgo la información que intercambiamos con la página web que estamos visitando. Esto sucede cuando se encuentra alguna vulnerabilidad en un navegador web, pero aún no se ha publicado el parche que la soluciona (esto es mejor conocido como fallo de día cero, para mayor información al respecto, consulta el artículo "Ataques al navegador," de esta revista).

Este lapso de tiempo es empleado por usuarios mal intencionados que intentan obtener datos personales (nombre, dirección, teléfono, por ejemplo) o sensibles (número de seguro social, número de cuentas bancarias, por ejemplo) de los usuarios.

Por lo anterior, cuando se emplea un navegador web, es necesario no ser sobre confiado de éste, independientemente del motor de renderizado y navegador que se utilice, ya que ninguno es cien por ciento seguro. Ante esta situación, es importante mantenerse informado sobre sus características principales. También es recomendable estar pendiente, tanto de actualizaciones como de vulnerabilidades existentes, para mantener una navegación más segura.

Existen sitios especializados en este tipo de información, como www.seguridad.unam.mx, en donde podemos encontrar las principales tendencias sobre estos temas.

Referencias:

Wikipedia: http://es.wikipedia.org/
W3C: http://www.w3schools.com/browsers/browsers_stats.asp
Flock: http://www.flock.com
Whatbrowser: http://www.whatbrowser.org/es/

Ataques al Navegador

Carmina Cecilia Espinosa Madrigal

Imagen 1. Navegadores web

El incremento de los sitios web y el fácil acceso a la información han convertido a los navegadores web en aplicaciones sumamente importantes y necesarias.

Los navegadores integran aplicaciones que permiten ampliar sus funcionalidades para soportar gráficos y todo tipo de animaciones. Razón por la cual muchos sitios web solicitan al usuario instalar programas adicionales para habilitar ciertas funciones, lo que implica un aumento en los riesgos de seguridad para los usuarios.

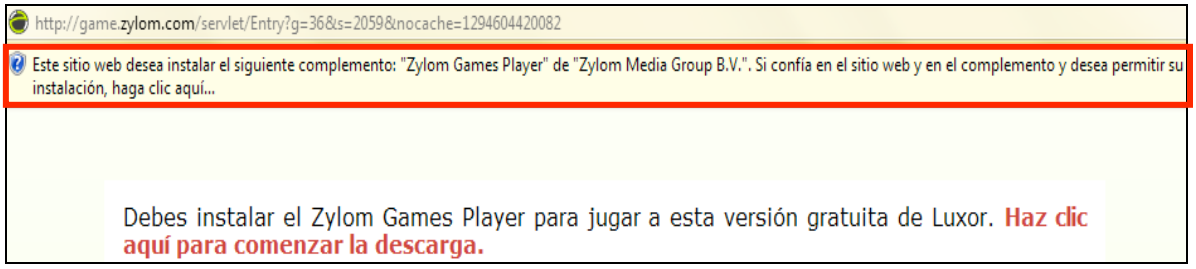


Imagen 2. Página web que requiere la instalación de un programa adicional para poder visualizar un juego.

El principal riesgo que existe al permitir la instalación de estas aplicaciones se debe a que el usuario puede descargar y ejecutar el programa sin estar consciente de lo que realmente sucede en su computadora.

Estas aplicaciones pueden provocar serios problemas en su equipo, causando daño a archivos, pérdida de datos y fugas de información privada.

Algunos ejemplos de dichas aplicaciones son *ActiveX*, *Shockwave*, *Java Applets*, *Javascript*, *Portable Document Format* (PDF) y *Flash*.

Existen distintos tipos de ataques originados por el mal uso de estas aplicaciones, por ejemplo:

- ***Tampering o Data Diddling***

Se refiere a la modificación no autorizada de la información. Por ejemplo, múltiples sitios web han sido afectados al detectar cambios en el contenido de sus páginas.

- ***Ataques Mediante JavaScript***

JavaScript es un lenguaje de programación usado por los diseñadores de sitios web. Este tipo de programas son utilizados para explotar fallas de seguridad de navegadores web y servidores de correo.

- ***Ataques drive-by download***

  Infectan de forma masiva a los usuarios, simplemente ingresando a un sitio web determinado. Mediante esta técnica, los desarrolladores de malware (programas maliciosos) propagan sus creaciones e inyectan código dañino entre su código original.

Los navegadores web se han convertido en el principal objetivo de usuarios mal intencionados, haciendo de estos herramientas de ataque.

Controles ActiveX

Los controles *ActiveX* forman parte de una tecnología de *Microsoft*, son pequeños bloques de programas diseñados para ser descargados y ejecutados por los navegadores web, además de ser usados para crear aplicaciones que trabajan sobre Internet. Entre los ejemplos, se incluyen aplicaciones personalizadas para la recolección de datos, visores para cierto tipo de archivos y para desplegar animaciones.

Algunos programas maliciosos pueden ocultarse en otros programas para atraer al usuario a descargar ciertas aplicaciones. Los controles *ActiveX* pueden ser adjuntados en un correo electrónico o descargados desde sitios web conocidos o no. Si una aplicación de *ActiveX* diseñada para actuar maliciosamente es descargada e instalada en el equipo del usuario, puede dañar el funcionamiento del sistema operativo del usuario, realizar cambio de contraseñas y robar información, por tal motivo se recomienda descargar programas sólo de los sitios web oficiales.

Para proporcionar cierta seguridad a los usuarios, *Microsoft* ha introducido un proceso electrónico para identificar al desarrollador del programa y proporcionar cierta seguridad de que el código no haya sido cambiado. Esto se realiza a través de firmas y certificados digitales, los cuales son sólo precauciones y no garantizan que el código sea seguro.

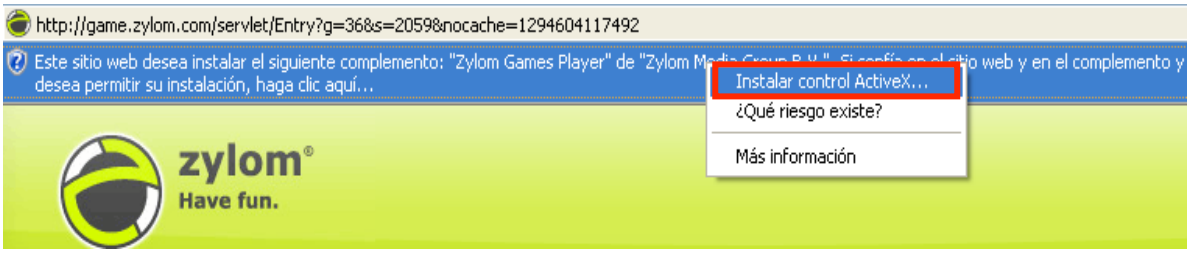


Imagen 3. Instalación de un control ActiveX solicitado por el sitio web.

Cuando el usuario accede a una página web que descarga un control *ActiveX*, se le preguntará si confía en la procedencia del control *ActiveX*. Si el usuario acepta el control, éste puede ejecutarse sin ninguna restricción. Con esto, la responsabilidad de la seguridad del sistema se deja en manos del usuario.

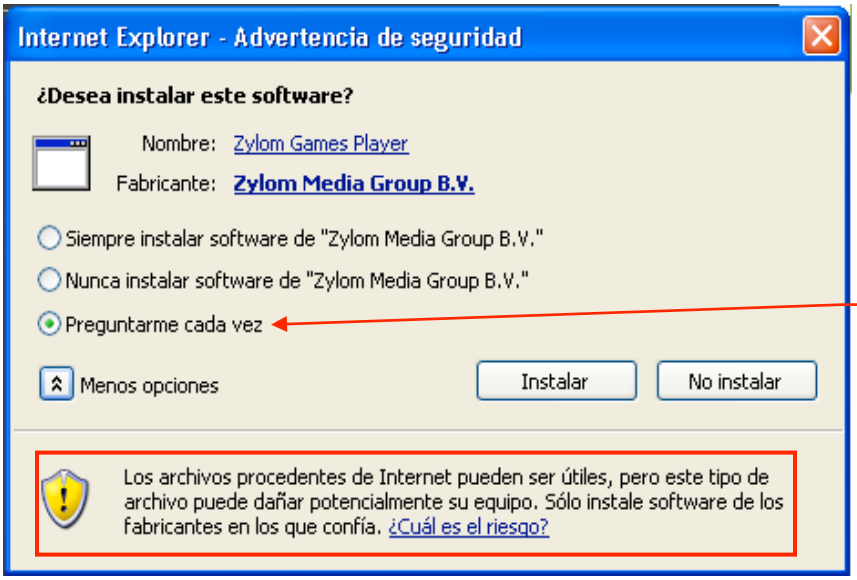


Imagen 4. Advertencia de seguridad al instalar un control ActiveX

Algunos controles *ActiveX* maliciosos manipulan el código de ciertos navegadores, para que éste no solicite confirmación al usuario a la hora de descargar otro control, dejando totalmente descubierto el sistema del usuario a ataques con tecnología *ActiveX*.

MITRE ha publicado poco más de 700 CVE "*Common Vulnerabilities and Exposures*" (http://cve.mitre.org/) con fallas de seguridad relacionadas a los controles *ActiveX*. Algunas de estas vulnerabilidades han sido calificadas con un nivel de riesgo ALTO, lo que significa que la falla de seguridad podría ser aprovechada para la ejecución de código remoto.

0-day en navegadores web

Los ataques conocidos como 0-day se aprovechan de las fallas de seguridad de un programa o sistema operativo que actualmente no cuentan con una solución, es decir, toman ventaja de fallas que no han sido reportadas al fabricante y por lo tanto la actualización para corregirlas no está disponible. Lleva el nombre de 0-day porque el ataque se produce antes del primer día en que la vulnerabilidad es conocida públicamente.

En el escenario ideal, cuando un investigador de seguridad encuentra una vulnerabilidad en algún programa, la reporta al fabricante, y éste se encarga de desarrollar una actualización que la corrija para finalmente publicarla y que los usuarios actualicen la aplicación.

Desafortunadamente, algunos hackers identifican las fallas de seguridad en las aplicaciones y las explotan antes de dar aviso. En algunos casos, se especula que gran parte de la información de las fallas de seguridad es negociada en privado dentro del mercado negro de vulnerabilidades sin

informar al fabricante del fallo, por lo que las actualizaciones no se crean dejando expuestos a riesgos desconocidos a los consumidores.

La Iniciativa de Día Cero de TippingPoint ZDI "*TippingPoint's Zero Day Initiative*" (http://www.zerodayinitiative.com/) es un programa que compra el derecho sobre la información de la falla de seguridad a cambio de la exclusividad de negociar las correcciones con los fabricantes afectados. La iniciativa ZDI es muy popular entre los hackers que buscan sacar provecho de sus investigaciones en un mercado legítimo.

Como una forma de presionar a los vendedores de software que postergan las reparaciones en las fallas de seguridad, a partir del 4 de agosto del 2010, *TippingPoint* estableció un límite de 6 meses para que las correcciones sean entregadas. Una vez que expire el plazo, se tiene previsto publicar un comunicado con algunos detalles sobre la falla y el programa afectado para ayudar a la comunidad a elaborar medidas de mitigación.

Algunos ejemplos de 0-day en navegadores web son:

- *Safari*

  En febrero de 2010, investigadores de seguridad encontraron ocho fallas de seguridad diferentes de día cero en el navegador *Safari* de *Apple*. Las fallas fueron calificadas de "alto riesgo" y vendidas a *ZDI*.
- *Firefox*

  En octubre de 2010, el equipo de *Trend-Micro* informó que el sitio web de los Premios Nobel había sido comprometido con la inserción de un código malicioso "*JS_NINDYA.A*" para propagar malware. La falla de seguridad desconocida afecta a *Firefox* 3.5 y 3.6.

Referencias:

http://kb.iu.edu/data/afoi.html
http://www.sans.org/reading_room/whitepapers/malicious/plain-english-risks-java-applets-microsoft-activex-controls_134
http://it-audit.sans.org/community/papers/internet-explorer-web-browser-security-review_170
http://www.addictware.com.mx/index.php/blog/580-asegure-su-navegador-web-
http://www.zonealarm.es/security/es/zonealarm-forcefield-browser-security.htm
http://www.sans.org/security-resources/10_security_trends.pdf
http://www.wisegeek.com/what-is-a-zero-day-attack.htm
http://threatpost.com/es_la/blogs/encuentran-vulnerabilidades-de-dia-cero-en-safari-030110
http://www.zerodayinitiative.com/advisories/upcoming/
http://threatpost.com/es_la/blogs/tippingpoint-decidio-establecer-un-limite-para-que-los-parches-de-seguridad-sean-entregados-08
http://www.youzone.es/2010/10/28/0-day-en-mozilla-firefox-explotado-activamente/

http://www.eset-la.com/centro-amenazas/1792-drive-by-download-infeccion-web
http://www.segu-info.com.ar/ataques/ataques_modificacion.htm
Imagen 1. http://geeksroom.com/wp-content/uploads/2010/04/navegadores1

David Eduardo Bernal Michelena

Las actualizaciones son porciones de software que distribuye un fabricante de software para corregir errores existentes en los programas, incluyendo a los navegadores, para extender o mejorar su funcionamiento, estabilidad y compatibilidad.

Cada fabricante tiene su propia clasificación de actualizaciones, pero en general podemos dividirlas en actualizaciones de seguridad y de funcionalidad. Las de seguridad tienen el propósito de corregir errores o vulnerabilidades, además se pueden subdividir en varios niveles de importancia según la gravedad de la vulnerabilidad que corrigen. Las más importantes son aquellas que permiten a un atacante remoto ejecutar comandos en el sistema comprometido, así como las que parchan vulnerabilidades de día cero.

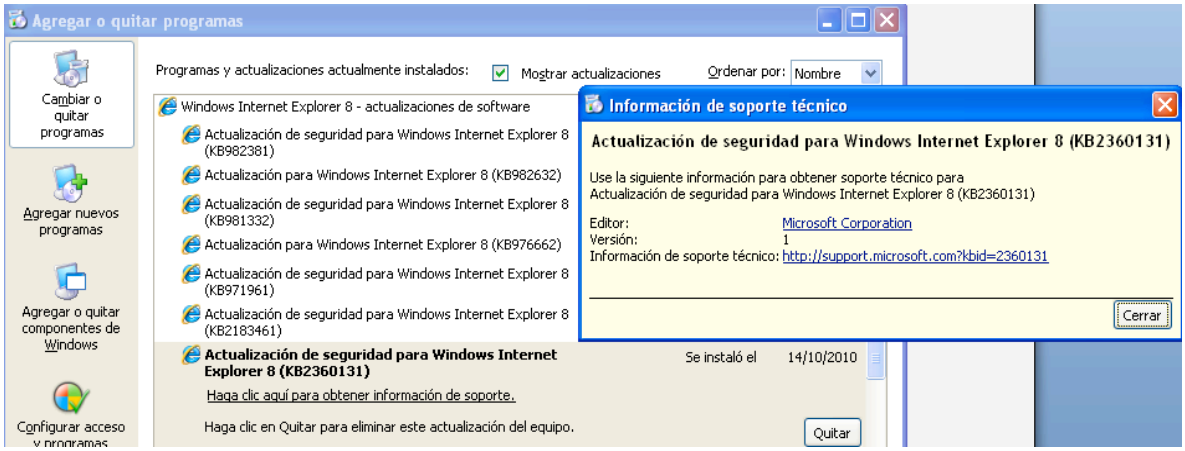
Si no se actualiza el navegador, se deja la puerta abierta para que alguna amenaza afecte nuestras computadoras y nuestra información, además de los problemas y limitaciones de funcionalidad, compatibilidad y eficiencia que tendrá nuestro navegador web.

Una de las organizaciones de seguridad más importantes en la investigación de vulnerabilidades de software, *Secunia*, publica un reporte anual que incluye pruebas y estadísticas de vulnerabilidades en los navegadores web más comunes.

En el reporte del 2009, se indica que la mayor parte de los exploits usados a gran escala, atacan vulnerabilidades viejas, presentes en las versiones desactualizadas de los navegadores. Según el reporte, el porcentaje de navegadores no parchados de *Firefox 3.0* fue de 17%, mientras que *Firefox 3.5* (la versión más reciente en el 2009) fue de sólo 9.3%. *Internet Explorer 6* registró 14.3%, mientras que *Internet Explorer 8* sólo presentó 3.6%. La tendencia es clara, un navegador actualizado significa menos vulnerabilidades y por lo tanto, menos probabilidad de que alguien afecte la seguridad de nuestro navegador.

Algunos fabricantes de software han implementado medidas para que sus programas se actualicen de manera automática, tal es el caso de *Microsoft*, con *Windows Update*, *Mozilla Firefox*, *Java*, *Flash*, entre otros. Cuando estos programas se instalan, levantan procesos que se conectan a sus servidores para buscar si hay actualizaciones disponibles, depende de la configuración, algunos las instalan automáticamente y otros presentan un botón de instalación al usuario final. Esto ayuda a que el software esté actualizado, ya que muchos no tienen la iniciativa o los conocimientos para descargar e instalar las actualizaciones manualmente.

Las actualizaciones de seguridad de *Internet Explorer* se pueden consultar en Agregar o quitar programas. Se selecciona Mostrar actualizaciones y luego se recorre la barra de desplazamiento hasta encontrar "*Windows Internet Explorer*". Si se desea ver información más detallada sobre alguna, se selecciona la actualización y el sistema muestra un cuadro de diálogo con una liga en la que podremos ver qué problemas específicos resuelve.

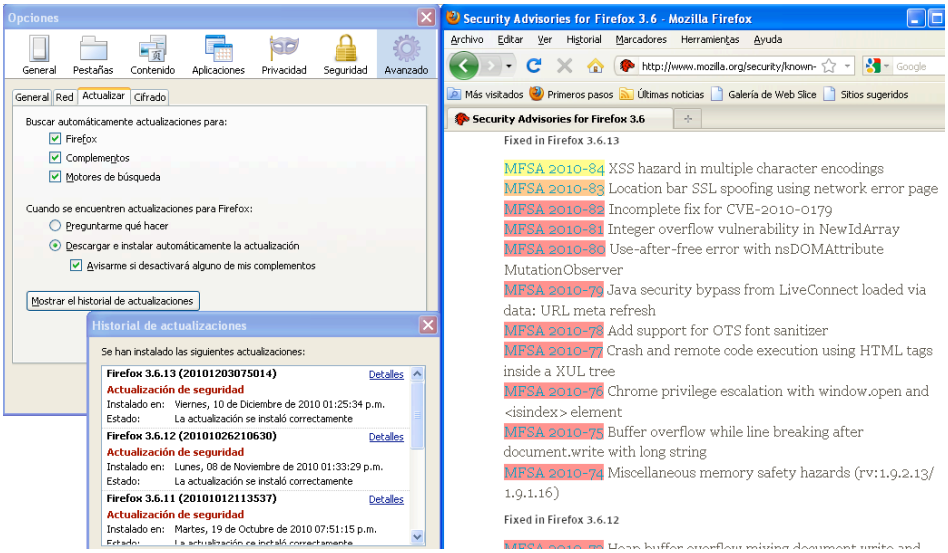


Para *Mozilla Firefox*, se tienen dos categorías de actualizaciones, las de seguridad y las de estabilidad. Las de seguridad corrigen vulnerabilidades en el software. Esta categoría a su vez se divide en tres:

- Crítico: Vulnerabilidad que puede ser utilizada para instalar software sin requerir interacción del usuario.
- Alto: Vulnerabilidad que puede ser usada para recopilar datos sensibles en ventanas o inyectando código, sin requerir nada más que acciones normales de navegación.
- Moderado: Vulnerabilidad que requiere que la víctima use configuraciones no predeterminadas o que ejecute una serie de pasos complicados o difíciles de realizar.

Estabilidad: Relacionadas con la funcionalidad, compatibilidad y estabilidad del navegador. En general, todos aquellos cambios no relacionados con la seguridad.

En este navegador podemos ver las opciones de actualización que tiene configuradas siguiendo la ruta: Herramientas>Opciones>Avanzado>Actualizar. Podremos ver las actualizaciones instaladas haciendo clic en el botón “Mostrar actualizaciones” que se encuentra en la parte inferior. Si se quieren ver los detalles que se corrigen, hacer clic en el vínculo “Detalles” ubicado en la actualización de interés:



Desgraciadamente la importancia de las actualizaciones es un arma de doble filo si no somos cuidadosos, ya que al instalarlas, en vez de incrementar su seguridad pasa lo contrario, comprometen sus equipos. La pregunta entonces es: ¿cómo distinguir las actualizaciones legítimas de las falsas que son usadas por los usuarios maliciosos para propagar su malware?

Simple, sólo descargar las aplicaciones y sus actualizaciones de los sitios de las organizaciones correspondientes. En algunos casos, como al utilizar *Internet Explorer*, sólo será necesario que tengamos habilitado *Windows Update* y la versión estable más actualizada del navegador se actualizará de forma predeterminada. Si se quiere actualizar inmediatamente, se debe descargar el programa de su página. Otros navegadores como *Mozilla Firefox, Google Crome* y *Opera* se actualizan automáticamente cuando se detecta una nueva versión, lo que permite que el usuario no se tenga que molestar descargando e instalando la actualización.

Para reducir el riesgo de instalar una aplicación maliciosa, se recomienda que los programas sean descargados directamente de la organización que los desarrolla y no de páginas de terceros, ya que versiones en otras páginas pueden ser versiones desactualizadas o peor aún, ser programas maliciosos que aparentan ser los navegadores.

A continuación se muestra una página de un tercero que permite descargar *Internet Explorer 7*, la cual indica incorrectamente que ésta es la versión más reciente del popular navegador web:

En caso de que la funcionalidad de actualización automática esté deshabilitada o por algún motivo no funcione, las actualizaciones también se deben descargar de la página oficial de la organización que las desarrolla. Para descargar los navegadores más populares, se debe hacer desde las siguientes URLs:

Mozilla Firefox:	http://download.mozilla.org/?product=firefox-3.6.13&os=win&lang=es-MX
Google Chrome	http://www.google.com/chrome/eula.html?hl=es
Internet Explorer (versión 8.0 estable)	http://www.microsoft.com/mexico/ie8/
Internet Explorer (versión 9.0 beta)	http://windows.microsoft.com/es-MX/internet-explorer/download/ie-9/worldwide
Opera:	http://www.opera.com/download/get.pl?id=33345&thanks=true&sub=true

Para saber si el navegador que estamos usando está en su versión estable más reciente, debemos consultar la página web del proveedor del navegador, dirigirnos a la sección de descargas y buscar el número de versión más reciente y luego compararlo con la versión de nuestro navegador, esto se puede consultar en Ayuda > Acerca de. Por ejemplo, para *Mozilla Firefox* haríamos lo siguiente: Entramos a http://www.mozilla.com/es-MX/firefox/ y comprobamos la versión más reciente (3.6.13):

Ahora verificamos cuál es la versión del navegador que estamos utilizando:

Algunos navegadores también permiten buscar actualizaciones en un solo paso, como es el caso de Mozilla por medio de su botón “Buscar actualizaciones” ubicado en el menú de Ayuda, pero el método explicado anteriormente es general para todos los navegadores.

Referencias:

http://secunia.com/gfx/pdf/Secunia_Annual_Report_2009.pdf
http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf
http://www.zdnet.co.uk/news/security-threats/2010/01/18/french-german-governments-warn-against-ie-39994504/

Las Extensiones del Navegador Web y sus Riesgos

Andrés Leonardo Hernández Bermúdez y Galvy Ilvey Cruz Valencia

La creciente necesidad de obtener más funciones del navegador es lo que dio origen a las extensiones, éstas pueden realizar tareas simples como buscar una palabra en un diccionario en línea o tareas más complejas como visualizar elementos del código fuente de una página para ayudar al desarrollo de la misma.

Los navegadores modernos soportan el uso de extensiones y cada uno define el formato en que éstas deben estar empacadas y organizadas para que se integren con el programa. Algunas son un archivo de tipo *zip*, con otra extensión mientras que otras son un archivo binario que se instala en el sistema. Las herramientas necesarias para desarrollar los archivos que forman parte de la extensión pueden llegar a diferir dependiendo del navegador sobre el que se vaya a trabajar.

Existen cinco navegadores que el *Consorcio World Wide Web* (*W3C*, por su acrónimo en inglés) reconoce como los más utilizados. Muchos de estos se pueden ejecutar en varios sistemas operativos. Estos programas son:

 *Mozilla Firefox*

 *Google Chrome*

 *Opera*

 *Apple Safari*

 *Microsoft Internet Explorer*

Principalmente, por número de usuarios, *Internet Explorer* y *Mozilla Firefox* son los más populares, por lo que abordaremos algunas de las extensiones más sobresalientes de éstos. *Firefox* es reconocido por ser un navegador con abundante uso de extensiones para mejorar la experiencia de navegación, entre las relevantes se encuentran:

1. **AdBlock.** Esta extensión de *Mozilla Firefox,* permite bloquear la publicidad de los sitios web, e incluso bloquea los dominios de malware, para que no aparezcan cuando se vuelva a abrir la página. Puede sitiar varios tipos de publicidad como flash, imágenes, java y scripts. En la interfaz se configuran suscripciones a listas que permiten identificar los elementos conflictivos y bloquearlos.
2. **CookieSafe.** Esta extensión de *Firefox* permite controlar los permisos de las cookies que se almacenan para diversos sitios web, el complemento puede permitir o denegar que un sitio web almacene cookies e incluso habilitar temporalmente que el sitio almacene cookies. Las cookies de la sesión actual se pueden exportar a un archivo *XML* para después importarlas y hacer uso de ellas. Se recomienda para una navegación más

segura deshabilitar globalmente las cookies y permitir de manera individual a cada sitio almacenarlas.

3. **Firefox Sync.** Esta extensión hace uso del servicio del mismo nombre que permite sincronizar los favoritos, el historial, los datos de formas y las contraseñas de los sitios. Los datos permanecen cifrados y sólo el usuario puede acceder a ellos.
4. **Session Manager.** Este complemento permite guardar las sesiones de navegación y guarda el estado de cada ventana por separado, se puede activar manualmente y además se activa cuando el navegador tiene algún problema y guarda la sesión para restaurarla cuando se abra de nuevo el navegador.
5. **Firebug.** Se utiliza para el desarrollo de páginas web. Permite analizar el código *HTML*, las hojas de estilo y los scripts de las páginas. Se pueden visualizar cambios en el estilo y en los elementos de forma instantánea, tiene una consola de errores para ver los fallos que tiene al cargarse la página e incluso mide el tiempo de carga de cada elemento de la misma.
6. **Screenshot Pimp.** Una vez instalada, esta extensión permite guardar capturas de los elementos de la página web o incluso de toda la página (no sólo de la parte visible en la ventana actual sino toda la página).

Por su parte *Internet Explorer*, aunque la mayoría de las extensiones (llamados componentes) están integradas al navegador, existen otras de terceros.

Dentro de las extensiones de terceros destacan:

- **Web slice.** Permite revisar automáticamente las páginas favoritas o partes de ellas, actualizará y notificará a los nuevos elementos que se agreguen en la barra de Favoritos.
- **Accelerator.** Realiza acciones para resaltar textos y direcciones electrónicas.
- **Buscador visual.** Presenta al usuario a través de sugerencias visuales, un resultado a su búsqueda mediante diferentes servicios web. Por ejemplo en barra de búsqueda, un usuario trata de localizar el nuevo "*Dell Streak*", y entonces alguna de las tiendas en línea, como *Amazon*, con sus herramientas de búsqueda ofrece entradas previas de los posibles modelos. No sólo las tiendas virtuales, también *Wikipedia* ofrecería esta ventaja sobre las entradas a un término solicitado.

Dentro de las propias, *IE* cuenta con extensiones aplicables a código *HTML*, *CSS* (hojas de estilo de cascada) y *DOM* (modelo de objetos del documento), "esto ha dado lugar a una serie de páginas web que sólo se pueden ver correctamente con *Internet Explorer*"[3], si se usa otro navegador podría abrir parcialmente o definitivamente no desplegarse. Sobresalen:

- **Internet Explorer Developer Toolbar.** Esta extensión sirve para validar páginas, de esta manera se determina lo que ocurre en el DOM, sobre todo al momento de ingresar a

[3] http://es.wikipedia.org/wiki/Internet_Explorer#Normas_de_extensiones

través de un *javascript*. Dentro de sus funciones sobresale que permite apreciar objetos HTML, como nombres, valores de pestaña y claves de acceso.

- **Web Accessibility Toolbar**. Se trata de una barra práctica de análisis que brinda la posibilidad de evaluar datos informativos sobre las páginas web que se visitan durante la navegación.
- **HttpWatch.** Ofrece medición sobre tiempos de carga, descarga, entre otra información sobre el nivel desempeño de un sitio.
- **WebCollect.** Esta extensión permite capturar imagen de una pantalla entera, al tiempo que brinda datos de dimensiones y pixeles, lo cual puede ser de utilidad al crear una pagina web.

Las extensiones propias pugnan por lograr una mejor experiencia de navegación en usuarios de Windows, ya que este navegador está pensado en el ambiente de ese sistema operativo. Incluso, Microsoft ha establecido que "los agregados pueden dar interesantes funcionalidades al navegador, pero también causar problemas de ejecución si no están bien escritos. La baja de velocidad en la navegación pude deberse también a éstos – especialmente al abrir una nueva pestaña"[4].

La idea es contradictoria, ya que *IE8* incluye la posibilidad de "importar extensiones de *Firefox*"[5] (ver fig. 1), la cual al final es sólo una llamada a buscar extensiones similares a éstas, y no específicamente las del otro navegador, acción que incurre hasta cierto punto en un engaño (ver fig. 2).

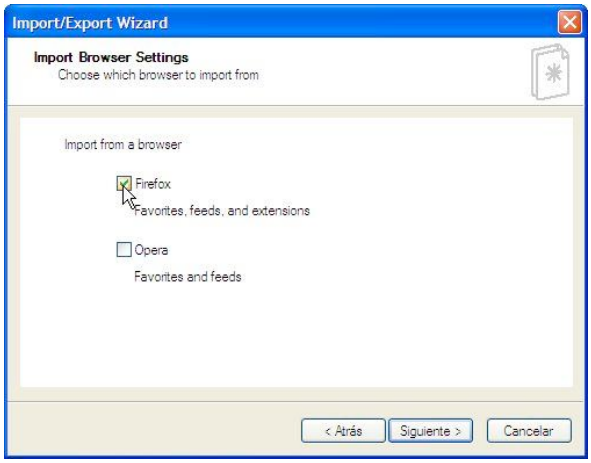


Figura 1

[4] http://bitelia.com/2010/04/microsoft-echa-la-culpa-de-problemas-en-ie-a-extensiones

[5] http://www.zonafirefox.net/2008/03/ie8-y-su-fraudulenta-importacion-de-extensiones.html

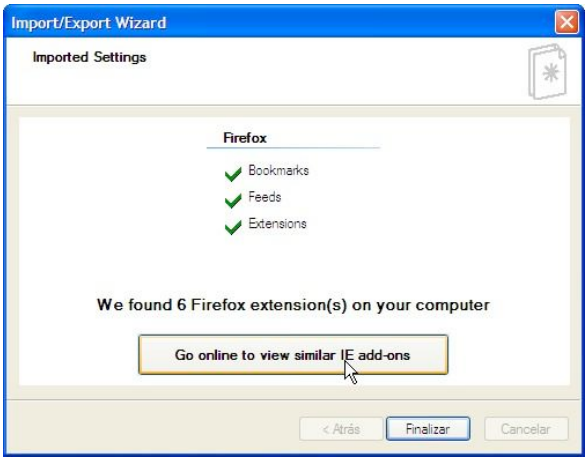


Figura 2

En la última versión, *IE9* (aún en beta), se pueden encontrar pocas extensiones, debido a que la mayoría de las mejoras ya están incorporadas[6]. Sin embargo, algunos terceros optan por proponer algunas todavía como es el caso de *FastestTube*, una extensión que sirve para descargar videos de YouTube, tal y como sucede con extensiones de *Mozilla Firefox* o Google *Chrome*.
Por lo que, la tentación por obtener estas extensiones y aplicarlas en el navegador muy probablemente continúe dando dolor de cabeza a los desarrolladores de Redmond.

Extensiones maliciosas

Los navegadores web aceptan las extensiones que el usuario descarga o instala sin verificar que éstas contengan algún malware, por ello, es altamente recomendable que el usuario sólo instale los agregados desde sitios oficiales, así como instalar software antivirus y antispyware en su equipo.
En algunas páginas maliciosas se ofrece descargar alguna extensión del navegador, dicho paquete contiene malware que puede infectar el equipo y causar problemas. Algunos sitios de descarga de archivos ofrecen instalar una barra de herramientas para "mejorar" la experiencia del usuario al utilizar el sitio, desafortunadamente muchas de estas contienen spyware, afectando tanto la navegación, como a la privacidad del usuario en línea, esto también aplica para los complementos ofrecidos al instalar algún programa *freeware* o *shareware* y para los programas "peer-to-peer" o *P2P*, como *ARES*.

Malware específico del navegador

Existe malware que toma ventaja de alguna capacidad del navegador (como las extensiones) e infecta el equipo, disminuyendo la velocidad de navegación, al mismo tiempo expone al usuario a

[6] http://ciberblog.wordpress.com/2010/10/21/descargar-videos-de-youtube-con-internet-explorer-9/

riesgos en línea. En 2008, se detectó un troyano (Trojan.PWS.ChromeInject) en una extensión del navegador *Mozilla Firefox*. Éste es el primer malware que saca ventaja del navegador y en 2010, la historia se repetiría, al detectarse otro troyano (Win32.LdPinch.gen) en la extensión *'Master Filter'* de *Firefox*.

Internet Explorer no es la excepción, en un listado del sitio *Tenebril*[7], se enumeran al menos doscientas supuestas extensiones que presumiblemente son programas spyware, los cuales pueden llevar el registro de la navegación que el usuario realiza. Por mencionar algunas de éstas:

- *AdBreak* y *Baidu Bar*. Extensiones, que una vez instaladas, permiten compartir información mientras se navega. Utilizadas principalmente por agencias publicitarias para registrar datos de clientes potenciales.

Las extensiones son una forma de mejorar y personalizar el navegador, la tarea pendiente, en todos los casos, es aprender a ser selectivos con los sitos desde los cuales se adquieran para no afectar al navegador, ni poner en riesgo información y equipos, además de evaluar la necesidad real de instalarlas.

Referencias:

Firefox Trojan Trojan.PWS.ChromeInject - Bitdefender
http://www.bitdefender.com/VIRUS-1000451-en--Trojan.PWS.ChromeInject.B.html
Firefox Phishing and Malware protection
http://www.mozilla.com/en-US/firefox/phishing-protection/
Firefox Pimp
http://ffpimp.com/?p=42
Firebug
http://getfirebug.com/whatisfirebug
Spyware self'-protection
http://www.getridofthings.com/get-rid-of-spyware.htm
Megaupload Toolbar is a Spyware which Changes Browser Settings - TheCredence.com
http://www.thecredence.com/?p=126
Extensiones de Terceros y propios IE
http://www.pcmag.com/article2/0,2817,2339704,00.asp
http://www.zonafirefox.net/2008/03/ie8-y-su-fraudulenta-importacion-de-extensiones.html
http://es.wikipedia.org/wiki/Internet_Explorer#Normas_de_extensiones
http://bitelia.com/2010/04/microsoft-echa-la-culpa-de-problemas-en-ie-a-extensiones
http://wjama.blogspot.com/2008/02/internet-explorer-developer-toolbar.html

[7] http://www.tenebril.com/src/spyware/internet-explorer-spyware.php

http://www.vuelodigital.com/2011/01/06/6-extensiones-de-internet-explorer-para-desarrollo-web/
Extensión descargar videos YouTube IE
http://ciberblog.wordpress.com/2010/10/21/descargar-videos-de-youtube-con-internet-explorer-9/
Extensiones maliciosas IE
Tenebril - Internet Explorer spyware
http://www.tenebril.com/src/spyware/internet-explorer-spyware.php

Israel Andrade Canales

Dado que el navegador web es una de las herramientas más versátiles en cómputo. Actualmente, esta tecnología es un lugar virtual recurrente para el fraude electrónico. Ello hace necesario adquirir hábitos que reduzcan el riesgo de ser víctimas de dichos fraudes y lograr una navegación confiable por la web.

A continuación se exponen algunas rutinas de navegación que pueden reducir de manera significativa el riesgo de fraude electrónico. Estos hábitos de navegación son buenas prácticas que se deben llevar a cabo en todo momento al navegar por Internet.

1. Gestión de Contraseñas

En la actualidad, los navegadores web tienen mecanismos para almacenar contraseñas (Ver Fig.1) de los sitios que requieren algún tipo de autenticación, esta funcionalidad es muy práctica para acceder a dichos sitios sin la necesidad de ingresar la contraseña de manera repetida. Sin embargo, el usuario debe ser capaz de gestionar sus propias contraseñas considerando lo siguiente:

1. Conocer los riesgos involucrados al adoptar estas funcionalidades, es decir hacer conciencia de que se están concentrando todas las contraseñas en un solo lugar.
2. No utilizar esta funcionalidad en todos los navegadores de Internet a los que accedemos, si se acepta el riesgo de utilizarla, debe usarse sólo en un navegador estrictamente personal, y no en uno público.
3. A veces, el uso frecuente del gestor de contraseñas ocasiona que no se recuerden las contraseñas o bien, que no se cambien las contraseñas recurrentemente, por lo que se debe ser consciente de esto y de vez en cuando ingresar la contraseña de manera manual.

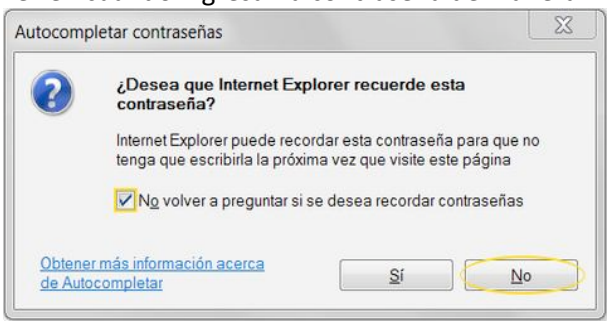


Imagen 1. Cuadro de diálogo de guardado de contraseña en Internet Explorer

2. Datos personales y la navegación en sitios públicos

La presencia extendida de los equipos de cómputo permite que se pueda acceder a diversos servicios a través de nuestro navegador web como centros de cómputo públicos, bibliotecas, escuelas, aeropuertos, etcétera, esto expone la información personal que queda registrada en el navegador a personas con las que se comparte el equipo de cómputo.

Para lo cual, la mayoría de los navegadores cuentan con funcionalidades de "navegación privada o segura" que impiden que se almacenen datos personales dentro del navegador como el historial de páginas vistas, esto es los rastros de nuestra navegación como imágenes, nombres de usuario y contraseñas estarán desapercibidos. **Es necesario conocer estas prestaciones y adoptarlas en nuestro hábito de navegación en sitios públicos.**

En la Imagen 1, se muestra el filtro para información privada *InPrivate* del navegador *Internet Explorer 9*, el cual permite realizar la navegación sin almacenar los rastros de navegación.

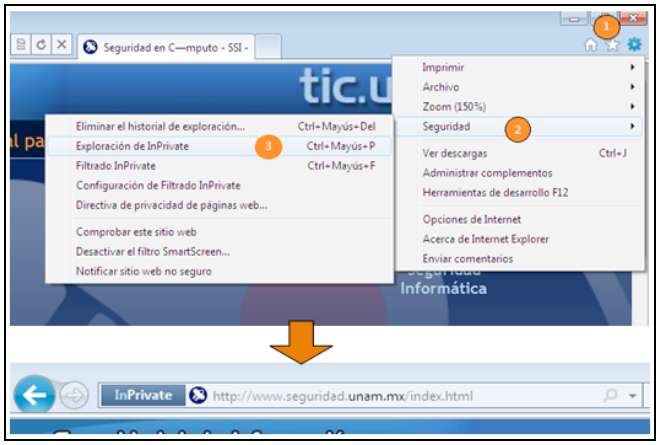


Imagen 2. Configuración del filtro InPrivate

En la Imagen 2, se muestra el filtro para información privada para *Firefox*, el segundo navegador más popular del mundo.

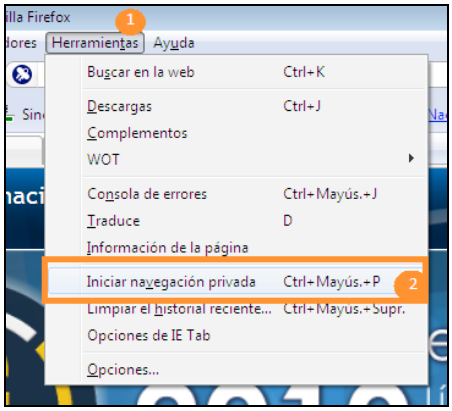


Imagen 3. Inicio de navegación privada para el navegador Firefox

3. Confianza de los sitios web

Hoy en día, gran parte del fraude electrónico se realiza a través de Internet, ataques, como phishing scam, se encuentran en la lista de ataques más realizados. Éste falsifica información de

algún servicio, de tal manera que el usuario envía información personal que cae en manos de los defraudadores.

Tan sólo en México, 1 de cada 850 sitios web es fraudulento[8], lo que significaría que el navegador ha llegado a ser un canal para realizar fraudes, por ello es muy importante conocer herramientas que ayuden a mitigarlo. Entre éstas se encuentran los calificadores de confianza de sitios web.
Estas herramientas calculan el grado de confianza de algún sitio de Internet a través de bases de datos de confianza generadas por usuarios o expertos, advirtiendo de posibles sitios fraudulentos o legítimos. Entre éstas se encuentran algunos complementos para el navegador como *WOT* y *Netcraft*, a continuación una breve descripción de ellos.

La herramienta *WOT* o Web De Confianza (*Web Of Trust*) es una base de datos de puntos de confianza en confidencialidad, fiabilidad del vendedor, privacidad y seguridad para menores implementada en páginas web calificadas por los usuarios que instalan la herramienta, además de utilizar los datos aportan su propia valoración. Esto permite al usuario que tenga esta herramienta conocer el grado de confianza asignado por otros usuarios. Dicha información es útil para identificar y bloquear los sitios con poca reputación, ya que la herramienta muestra una advertencia antes de lanzar la página. En la imagen 3, se muestra un ejemplo de su funcionamiento.

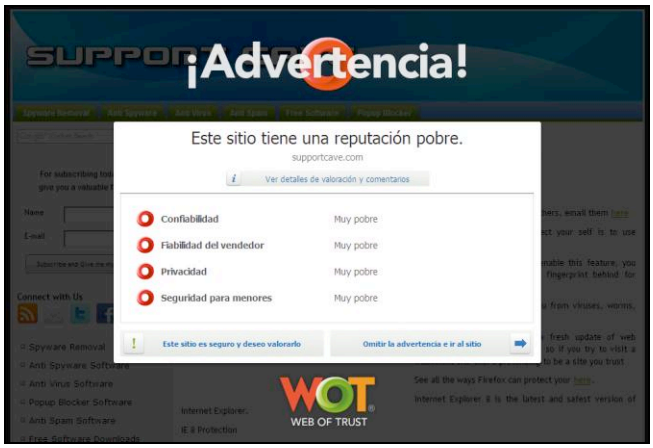


Imagen 3. Advertencia de un sitio con poca reputación antes de que sea completamente visible.

Otra herramienta que permite obtener una calificación útil para evaluar si el sitio es peligroso, es la barra de herramienta *Netcraft*. Esta herramienta califica el riesgo de la página al evaluar la reputación del servidor que la hospeda, la dirección de Internet, entre otras para mostrar el valor de riesgo (Imagen 4).

[8] http://toolbar.netcraft.com/stats/countries

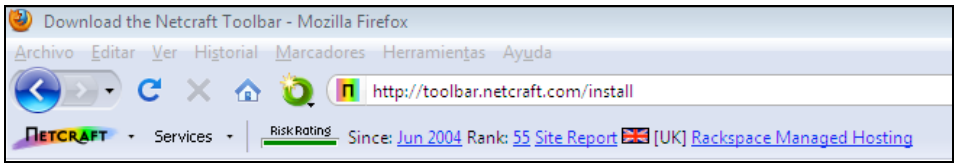


Imagen 4. Barra de herramientas Netcraft evaluando el riesgo del sitio. Cuando la línea se encuentra en rojo se indica un riesgo alto de fraude.

4. Cuida de tu navegador: actualízalo y evita que lo modifiquen.

Algunos fraudes electrónicos a través del navegador aprovechan debilidades en su diseño, esto es porque éste es un software muy complejo que consta de varios cientos de miles de líneas de código suseptibles a errores. Por lo que una adecuada práctica de navegación confiable incluye la actualización frecuente de dicho navegador.

Es importante estar conciente del navegador que elegimos. Actualmente el navegador más popular es *Internet Explorer 8*, seguido de *Firefox*[9]. Por lo que se puede suponer que la mayoría de estos navegadores son el blanco para aprovechar las vulnerabilidades del navegador.

Por otra parte, es importante evitar el uso de software ilegal o procedente de sitios de reputación pobre debido a que pueden alterar de manera nociva el funcionamiento del navegador con la finalidad de interceptar información personal o redirigir el tráfico a sitios fraudulentos.

Además, es común que las ligas de descarga de música, imágenes o videos ilegales redirijan a software maliciosos, ya que esta es una forma común que los defraudadores de distribuir el malware. Es muy importante obtener los archivos de fuentes legítimas y legales.

5. Navegar en sitios seguros.

Las primeras tecnologías de Internet no contemplaron la transmisión segura de información. Esto generó la integración de nuevas tecnologías como el *protocolo https*, el cual establece mecanismos para proteger los datos durante su transmisión. Esta tecnlogía es utilizada ampliamente en el comercio electrónico para el intercambio de datos como tarjetas de crédito, consultas hacendarias, de seguro social, académicas,etc. El navegador web debe informar del uso de esta tecnología tomando encuenta algunos puntos importantes:

Generalmente indicará que se ingresa o se deja un sitio seguro (esto quiere decir que los datos transmitidos van protegidos o no).

Imagen 5. El navegador pondrá en la página el protocolo https y en la parte inferior (parte derecha de la imagen) indicará la autoridad de confianza que certifica al sitio.

Demostrará si el sitio cuenta con un certificado válido o no, el cual es la prueba ante una autoridad

[9] http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0

de confianza si el sitio es legítimo y que los datos viajarán de manera confiable o no.

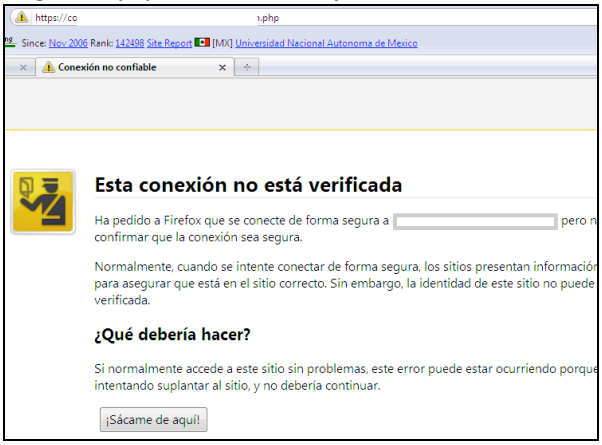


Imagen 6. El navegador Firefox advierte que el certificado no esta certificado por una autoridad de confianza.

6. Oculta tu rastro de navegación

Al navegar en Internet compartimos información con los sitios a los que accedemos, entre ésta destacan los datos del navegador que utilizamos, el sistema operativo o la dirección de Internet desde la cual accedemos (Imagen 7). Dicha información puede ser utilizada por software malicioso para recuperar información de nuestros equipos y explotarla. Una solución son los proxies, éstos son equipos intermediarios a través de los cuales los detalles de nuestra navegación cambian ocultando los reales.

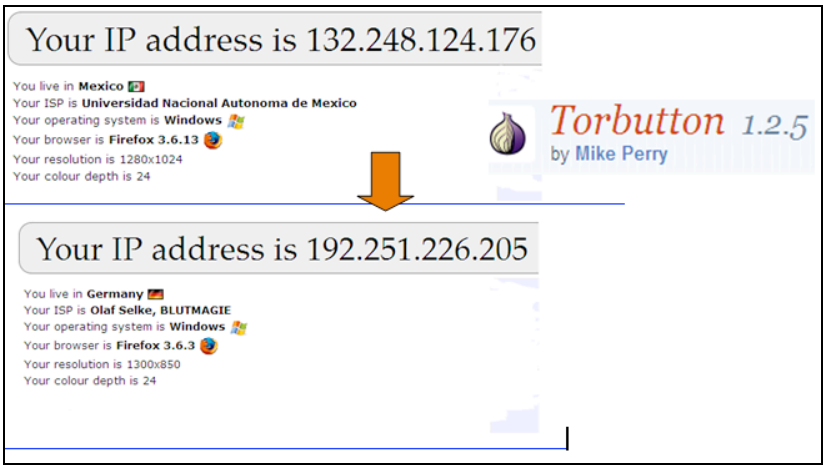


Imagen 7. El plug-in de Firefox , Torbutton, funciona como proxy para ocultar los datos que el navegador transmite a los sitios de Internet.

Estos consejos permiten reducir considerablemente el riesgo de ser víctimas de fraude electrónico a través del navegador. Para más información de este y otros temas de seguridad informática, la

Subdirección de Seguridad de la Información pone a disposición de los lectores sitios como información relevante en: http://www.seguridad.unam.mx

Referencias:

http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0
http://toolbar.netcraft.com/stats/countries

Andrés Velázquez*

Cada día se escucha más sobre la posibilidad de ser defraudado por medio de Internet, de la posibilidad de que un empleado haya robado información confidencial o un secreto industrial dentro de la empresa en la que labora. El cómputo forense, una disciplina relativamente nueva, ha servido como una herramienta reactiva para poder determinar qué y cómo sucedieron los ejemplos anteriores. Esto nos hace recordar aquella excelente frase del profesor Eugene Spafford: "El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de Titanio, encerrado en un búnker de concreto, rodeado por gas venenoso y cuidado por guardias muy armados y muy bien pagados. Aun así, no apostaría mi vida por él".

Y es que no es un secreto, ni una situación de telenovela, que en países de América Latina los fraudes –haciendo uso de la tecnología- se han incrementado. Simplemente, recuerdo un par de casos en los cuales hemos estado involucrados: contadores que no pagan correctamente los impuestos y realizan transferencias a números de cuenta bancarios de un familiar; personal de almacén coludidos con proveedores para recibir mercancía defectuosa, gracias a los mensajes de texto (SMS) que intercambian entre ellos; el empleado que antes de renunciar decide conectar una memoria de USB para respaldar su información y de paso la base de datos de los clientes de la empresa; hasta la ya tradicional amenaza vía correo electrónico.

Las tendencias son claras, hacemos más uso de la tecnología para diferentes situaciones dentro de nuestra vida diaria: pago de impuestos, transferencias interbancarias, llamadas y mensajes de texto desde nuestros celulares y muchas otras cosas más. Sin embargo, esa misma tecnología también se está usando para poder obtener un provecho, el cual no recuerdo haber escuchado o discutido con alguien un par de años atrás, y menos mientras estudiaba mi carrera en la universidad.

La seguridad de la información es un elemento clave y preventivo que nos permite disminuir el riesgo de que alguna situación, como las que acabo de mencionar, pueda explotar dentro de la organización; aunque normalmente se considera desde una perspectiva de "protegernos de los externos", hay una situación importante que pocas veces se toma en cuenta: LOS INTERNOS; aquellas personas que se encuentran dentro de la organización, y quienes tienen acceso con un simple clic a la información, hacen buen o mal uso de la infraestructura y cuentan con acceso a casi todo lo que hace que sea considerada "una organización".

Si consideramos lo anterior, sería más común de lo que actualmente se hace, encontrar políticas internas del uso de Internet y del correo electrónico corporativo; así como firewalls internos; cartas de asignación de equipos de cómputo, teléfonos celulares y contratos de confidencialidad que establezcan claramente la protección a la información en formato digital.

Cuando toda salvaguarda, control y elemento de seguridad implementado de forma preventiva no permite detener o evitar un incidente, es momento de incorporar al cómputo forense para poder determinar qué paso y aprender del mismo. Muchas son las organizaciones que simplemente contienen y reparan –lo cual no digo que esté mal-; no obstante, tiene mucho más valor el aprender y resolver de tal manera que el incidente no vuelva a pasar, o que en caso de ocurrir, deje la información suficiente para poder reaccionar.

Pero, ¿qué se necesita para poder crear un laboratorio de cómputo forense dentro de una organización?

La respuesta en sí, muchas veces es compleja, porque depende de muchos factores; sin embargo, se requiere de recursos humanos, hardware, software y procedimientos a la medida para poder atender los tipos de casos según la organización. Los recursos humanos no necesariamente tienen que estar dedicados al 100% a esta actividad, pero si requieren de un proceso de capacitación y entrenamiento continuos para poder reaccionar al nivel requerido de la organización. El resto de elementos sí debe ser dedicado y a la medida para poder reaccionar correctamente. No es lo mismo un laboratorio que realizará únicamente análisis a equipos Windows, que si requiere analizar diferentes sistemas operativos o teléfonos celulares.

Los procesos deben cumplir con las mejores prácticas internacionales en la disciplina, como el sobrescribir (wipe) todo disco duro antes de usarlo, a fin de confirmar que no tiene ningún elemento que pueda comprometer la imagen forense -copia bit a bit del contenido de un medio de almacenamiento- que se va a generar. Los formatos de cadena de custodia, de adquisición de evidencia y de seguimiento son parte de los procedimientos para poder tener control de cada uno de los elementos que se analizarán. Y es que, aunque un análisis forense se realice de forma interna, es imprescindible contar con elementos de integridad que permitan proteger a quien realiza el cómputo forense, y así, éste no se vea involucrado en una acusación.

Son muchos los retos a los cuales se enfrenta el cómputo forense, van desde el cambio constante de la tecnología, que requiere de la atención continua por parte de los investigadores para poder conocer y saber a lo que se enfrentan, así como al uso del *cloud computing* y los procedimientos para poder realizar análisis sobre ellos hasta el tiempo de procesamiento de discos duros de grandes capacidades.

El cómputo forense es una gran herramienta, tanto para realizar investigaciones internas como para poder usarlo para un procedimiento legal.

**Andrés Velázquez*, CISSP, GCFA, IEM, ACE, Presidente y Director de Investigaciones Digitales de MaTTica, el primer laboratorio dedicado a la investigación de delitos informáticos en América Latina con presencia en México y Colombia.

DIRECTORIO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dr. José Narro Robles
Rector

Dr. Sergio Alcocer Martínez de Castro
Secretario General

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Dr. Ignacio de Jesús Ania Briseño
Director

MTIA. Oscar Fernández Berdejo
Director de Telecomunicaciones

Ing. Rubén Aquino Luna
Subdirección de Seguridad de la Información
UNAM-CERT

Revista elaborada por la
Dirección General de Cómputo y de
Tecnologías de Información y Comunicación

CRÉDITOS
PUNTO SEGURIDAD, DEFENSA DIGITAL

Galvy Ilvey Cruz Valencia
Edición

Angie Aguilar Domínguez
Carmina Cecilia Espinosa Madrigal
David Eduardo Bernal Michelena
Andrés Leonardo Hernández Bermúdez
Galvy Ilvey Cruz Valencia
Israel Andrade Canales
Participación especial: Andrés Velázquez
Colaboraciones

Ing. Rubén Aquino Luna
Subdirección de Seguridad de la Información
UNAM-CERT

Galvy Ilvey Cruz Valencia
Jesús Mauricio Andrade Guzmán
Revisión de Contenidos

Act. Guillermo Chávez Sánchez
Coordinación de Edición Digital

Diana Chávez González
Coordinación de la Producción Digital

Lic. Lizbeth Luna González
Dolores Montiel García
L.D.C.V. Carolina Silva Bretón
Diseño Gráfico

Liliana Minerva Mendoza Castillo
Formación

2011 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Cómputo y de
Tecnologías de Información y Comunicación