Webs que nos espían

Un estudio de la Universidad de Princeton señala que 500 páginas web de las más populares del mundo emplean *scripts* que les permiten registrar cada *clic* y cada palabra escrita por los usuarios y enviar la información a un servidor de terceros. Los expertos recomiendan utilizar navegadores que ofrecen anonimato y privacidad, usar redes privadas virtuales o instalar *pluggins* para bloquear estos programas.

LUIS MENÉNDEZ

luis.menendez@yahoo.es

¿Debemos resignarnos?

'PARA nada', zanja Eduardo Sánchez, CSO de onBranding. "Tenemos que aprender a cambiar la manera de navegar. Podemos utilizar navegadores que ofrecen anonimato y privacidad, usar redes privadas virtuales, conocidas por sus siglas VPN, o instalar *pluggins* en el navegador para bloquear estos programas." Este experto nos anima a poner cada vez más capas, no solo de seguridad sino de privacidad. "Al igual que en casa tenemos cortinas, hay que intentar poner en internet todas las capas necesarias para preservar nuestra privacidad."

CUALQUIERA QUE HAYA navegado por internet sabe, o al menos intuye, que muchas de las páginas web que visita recaban información de sus movimientos y le reconocen si vuelve a consultar la misma página. Pero una cosa es eso y otra bien distinta es que registren cada tecla que pulsa en el teclado del ordenador, si rellena un formulario, e incluso si escribe algo y posteriormente decide borrarlo.

Un estudio en el que han intervenido tres investigadores del Centro de Política de Tecnología de la Información de la Universidad de Princeton revela que cerca de 500 de las páginas web más populares del mundo registran cada golpe de teclado y posteriormente envían esa información a un servidor de terceros.

Los responsables de recopilar esta información son los llamados "*scripts* de reproducción de sesión", que suelen ser utilizados por las empresas para obtener información sobre cómo sus clientes utilizan sus sitios y para identificar páginas web confusas o con errores de diseño. Este *software*, según el informe, no solo recoge estadísticas generales sino que sería capaz de grabar y reproducir sesiones de exploración individuales.

¿Qué son los *scripts*? Los *scripts* no se ejecutan en todas las páginas pero, según los investigadores, a menudo se colocan en páginas donde los usuarios aportan contraseñas o datos de carácter médico. "La recopilación de contenido de la página por parte de *scripts* de reproducción de terceros puede hacer que la información sensible, como las condiciones médicas, detalles de la tarjeta de crédito y otra información personal mostrada en una página, se filtre a terceros como parte de la grabación", recuerdan.

Uno de los hallazgos más inquietantes de la investigación es que algunas de las compañías que ofrecen este *software*, como FullStory, diseñan *scripts* que incluso permiten a los propietarios de sitios web vincular las grabaciones que reúnen con la identidad real de un usuario. Esto se traduce en que las empresas pueden ver que un usuario está conectado a un correo electrónico o nombre específico.

"Los *scripts* de reproducción de sesión están programados de forma que son capaces de grabar o identificar

los movimientos que hace el usuario", señala Lorenzo Martínez, CTO de Securízame. "Cuando visitas la página se ejecutan acciones en tu navegador que envían al servidor lo que tú vas haciendo."

Estas aplicaciones o pequeños programas son utilizados en el campo del marketing digital para hacer análisis web. Los desarrolladores examinan si las personas que navegan en una determinada página llegan hasta abajo con el *scroll* y ven todos los productos o si se cansan; observan dónde han pinchado en cada una de las veces por si la web no es suficientemente intuitiva. Con esta información elaboran perfiles de usuario de manera anónima y en función de eso generan una analítica para saber si la web funciona o el tipo de usuario que navega.

Recursos para proteger nuestra privacidad

▶ Para forzar a los navegadores a conectar con páginas https: HTTPS Everywhere.
▶ http://cort.as/-7iuW

▶ Para evitar rastreos: Privacy Badger o similares.
▶ http://cort.as/-7iuu

▶ Complemento para inhabilitación de Google Analytics y evitar el rastreo de cookies en las webs que lo tengan habilitado.
▶ http://cort.as/-7itK

▶ Bloqueadores de publicidad: uBlock Origin, Adblocker ultimate, AdBlock Plus y AdBlock

A través de una web con este tipo de *script* se puede obtener bastante información, no solo dónde clican o el perfil de usuario. Si visitamos una página web, independientemente de cual sea, a esa página web le estamos diciendo a qué navegador accedemos, y cuál es su versión; nuestro sistema operativo y dispositivo de acceso; la dirección IP que estamos utilizando; si tenemos activos Javascript, Flash, etc… "Se hace un *fingerprinting web*: si vuelves a navegar con el mismo dispositivo y navegador se genera una huella del usuario que te identifica de manera unívoca, de forma que no saben cómo te llamas pero sí que tu usuario puede visitar la web varias veces", explica Eduardo Sánchez, CSO de onBranding.

Lorenzo Martínez: 'Los *scripts* de reproducción de sesión están programados de forma que son capaces de grabar o identificar los movimientos que hace el usuario'

Por su parte, Google cuenta con su herramienta Analytics, a través de la cual es posible saber, entre otros datos, el número de usuarios que han visitado una página web o desde dónde se lleva a cabo la visita, ya que la dirección IP desde la que se realiza la visita informa automáticamente desde dónde se está haciendo. Esta información es útil para hacer estudios de mercado y conocer, por ejemplo, cuáles son los productos o servicios más visitados y desde dónde. "En

marketing se utiliza para mejorar las ventas", aprecia Sánchez.

En otros casos el interés es identificar el tipo de usuario que entra o cuántas veces lo hace. Es muy común –e irritante– consultar una página web para encontrar un vuelo y, al volver a acceder a dicha página una segunda o tercera vez, comprobar que el precio del vuelo se ha incrementado. Las *cookies* detectan cada vez que entramos y saben que somos el mismo usuario que se estuvo interesando por un vuelo recientemente.

Mapas de calor

EXISTE *software* de estadísticas, como Open Web Analytics, capaces de saber cada movimiento que hacemos al visitar una página web. Alejandro Ramos, experto en seguridad informática y actual CISO de Telefónica, lo ilustraba con un ejemplo en un taller técnico celebrado en una edición pasada de CyberCamp. Ramos rellenó de forma ficticia un formulario para interesarse por una casa rural que no llegó a enviar. A continuación, accedió a una funcionalidad de este *software* de estadísticas, llamada *domstreams*, capaz de reproducir, como si de una película se tratara, todos los movimientos y pulsaciones de teclado efectuadas. "Es como un *software* espía que ofrece la capacidad de saber qué ha escrito un usuario que ha cumplimentado un formulario incluso si no ha llegado a enviarlo. De hecho, sería capaz de registrar aquello que hemos escrito aunque nos hubiéramos arrepentido y lo hubiéramos borrado", subraya Ramos. El objetivo de estas herramientas es, como indica este experto en seguridad informática, la elaboración de mapas de calor para conocer por dónde pasa el ratón el usuario, qué textos selecciona o cuál es la parte más importante de esa web para situar ahí una oferta o promoción.

"Hay complementos que te permiten evitar la ejecución de determinados códigos maliciosos en tu navegador en algunos casos, pero que en otros evita que funcione correctamente un sitio web", afirma Lorenzo Martínez. En esta línea se muestra Eduardo Sánchez, para quien estos *scripts*, que utilizan código Javascript, se pueden bloquear con extensiones que se añaden al navegador. Sin embargo, hay otras webs que cuando entras te dicen que tienes que deshabilitar el programa que está bloqueando los *scripts* porque de no hacerlo no puedes navegar en esa web. "Lo que quieren es obtener la máxima información posible tuya, no solo darte una experiencia de usuario final atractiva mediante esos *scripts*."

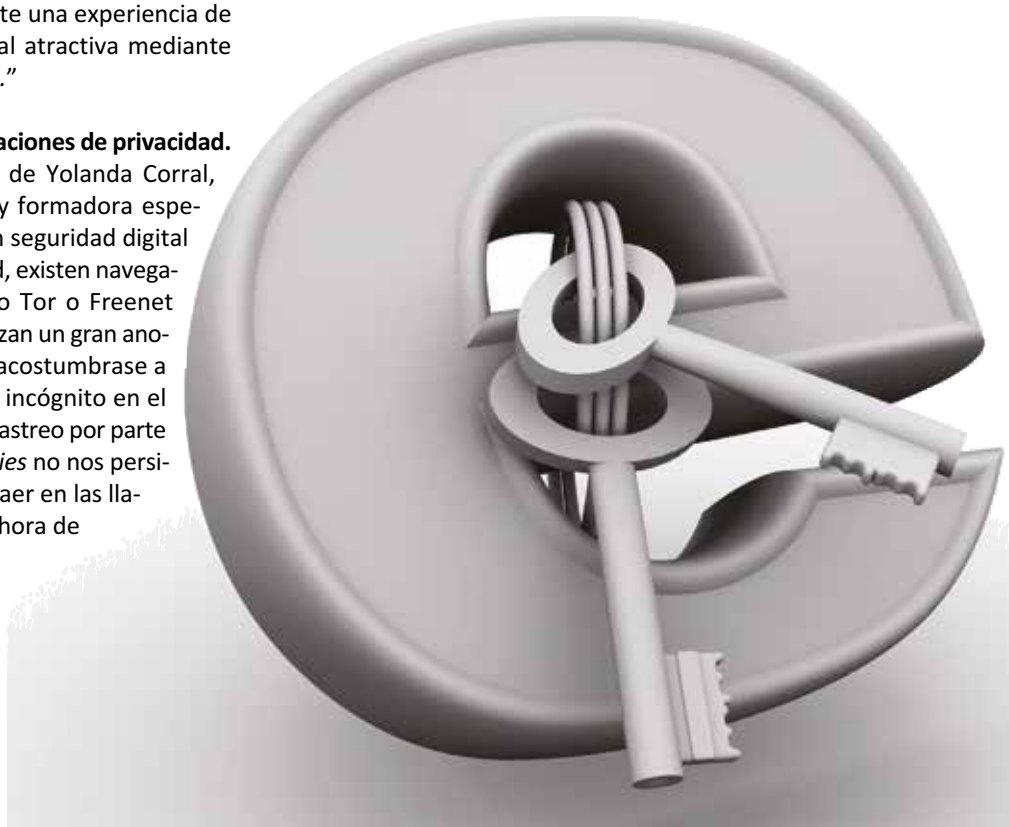
Recomendaciones de privacidad. En opinión de Yolanda Corral, periodista y formadora especializada en seguridad digital y privacidad, existen navegadores como Tor o Freenet que garantizan un gran anonimato. "Aunque bastaría con acostumbrase a navegar de modo privado o de incógnito en el navegador habitual para que el rastreo por parte de terceros sea menor, las *cookies* no nos persigan al cerrar la sesión y evitar caer en las llamadas 'burbujas de filtros' a la hora de buscar información."

También existen extensiones en el navegador para limitar la publicidad, notificar a las webs que no queremos ser rastreados o para forzar la navegación por el protocolo https, que hace que la navegación sea segura y cifrada de punto a punto, entre otros fines. Asimismo, Corral aconseja limpiar de forma cotidiana el historial y las *cookies* en el navegador, incluso accediendo a la configuración para que se borren al cerrar sesión.

Yolanda Corral: 'Bastaría con acostumbrase a navegar de modo privado o de incógnito en el navegador habitual para que el rastreo por parte de terceros sea menor'

Eduardo Sánchez: 'Los *scripts* se pueden bloquear con extensiones que se añaden al navegador, pero hay otras webs que obligan a deshabilitar los bloqueadores para poder navegar en ellas'

Además, considera muy recomendable hacer la revisión de Google en "mi cuenta" o "mi actividad" para configurar la privacidad y los permisos de Google en el rastreo del historial de navegación, vídeos vistos, ubicaciones o la información que comparte con terceros. "Todo aquel que tenga una cuenta en Google debe invertir unos minutos en revisar siempre este panel y en las redes sociales que tenga perfil también." ●



CARMELO ENCINAS,
periodista

carmeloencinas@hotmail.com
@CarmeloEnc

Intimidad, ¿para qué?

CON LA INTIMIDAD OCURRE un poco como con la libertad, que realmente solo valoramos su importancia cuando nos la quitan. Bien es verdad que no a todos les preocupa proteger su vida íntima, mucha gente incluso la airea constantemente para satisfacer su vanidad o por la necesidad de llamar la atención y sentirse protagonista de algo. Luego están los casos extremos, aquellos que convierten su vida personal y sus relaciones amorosas en un espectáculo público con el objeto de monetizarlo. Es obvio que estos últimos pierden ante la sociedad el derecho, que a todo a ser humano se le atribuye, de que nadie meta las narices en su intimidad.

Personalmente me produce cierta indignación la actitud de esos personajes de pacotilla que sin otro mérito conocido que el de sus relaciones de cama se lamentan del acoso de los paparazzi después de haber rentabilizado su inmerecida fama. Cuando uno abre la puerta de sus interioridades a la indiscreción ajena ha de saber lo que arriesga y cuáles pueden ser las consecuencias de despertar curiosidades insaciables.

Es una lección que deberían aprender igualmente aquellos que utilizan las redes para difundir fotos y comentarios en voz alta que dejan al descubierto toda suerte de intimidades y que ahí quedan flotando para uso y disfrute de fisgones, incluidos los más indeseables. Tendría que haber en las escuelas una asignatura complementaria que aleccionara a los chicos sobre los peligros que comporta para ellos y sus familias una utilización banal de internet y cómo hacer para navegar de forma responsable. Es una materia que deberíamos aprender también los adultos que, con frecuencia, operamos en la Red sin la menor idea de dónde puede ir a parar lo que tan generosamente insertamos.

Ese aparato que ya todos llevamos en el bolsillo y al que llamamos teléfono móvil, cuando en realidad es un completo ordenador que nos permite realizar cualquier operación, es además un pequeño y eficaz espía. No solo registra todos nuestros mensajes y conversaciones; también los movimientos que hemos realizado y dónde nos hallamos en cada momento. Eso puede ocurrir, aunque esté apagado y solo al retirar la batería se desactiva su capacidad de escudriñarnos.

Siempre me llama la atención el que un conocido político, que ocupó con eficacia el Ministerio del Interior, siga utilizando un teléfono móvil de los antiguos sin conexión posible a la Red. De igual forma, cada vez es más frecuente que para entrar en determinados despachos oficiales o reuniones de alta dirección sea preceptivo dejar el móvil antes de cruzar la puerta. Nadie, sin embargo, renunciaría ya a las ventajas y comodidades que proporcionan estos dispositivos que nos permiten, además de comunicar y mensajear, obtener información y realizar operaciones complejas, en cualquier situación y desde cualquier lugar.

"El ruido también mata"

Nuestra confianza en el sistema llega a tal extremo que el comercio electrónico se prevé capaz de revolucionar el mercado proyectando un escenario económico en el que la recopilación y el manejo de datos sobre los consumidores resulta estratégico. Y cuando hablo de datos, me refiero a nuestros datos, datos personales identificables que pueden revelar gustos, aficiones, información médica y también detalles de tarjetas de pago, que son archivados y procesados por empresas que controlan los comportamientos de navegación.

Un estudio realizado meses atrás por la Universidad de Princeton revela que hay cientos de páginas digitales que realizan por sistema un seguimiento de cada movimiento de *ratón* y de cada pulsación de tecla, y cómo cualquier información introducida por el navegante es registrada antes incluso de ser enviado el formulario.

La conclusión del estudio es que hay un gran negocio montado en torno al rastreo de datos que vulnera las normas sobre privacidad. Las páginas digitales que adquieren esa información lo justifican argumentando que lo hacen para mejorar la experiencia del usuario, es decir para ofrecerle de forma selectiva aquello que más le puede interesar, pero lo cierto es que violan nuestro derecho a la intimidad.

«Un estudio revela que hay cientos de páginas digitales que realizan por sistema un seguimiento de cada movimiento de *ratón* y de cada pulsación de tecla»

Empieza a haber un rechazo considerable a esta suerte de "gran hermano" que se refleja en el hecho de que cada vez haya más gente ejercitando el llamado *dirty data* y que no es otra cosa que proporcionar datos falsos cuando se interactúa con las páginas web de las empresas. Esta práctica es ya tan frecuente que calculan que uno de cada cuatro datos proporcionados por los usuarios, cuando realizan operaciones a través de internet, es deliberadamente erróneo. Quienes lo hacen es casi siempre para evitar ser identificados y burlar el acoso de la publicidad *online*. En lo que más se suele mentir es en la edad y en la localización geográfica para así ser excluidos o incluidos en determinados segmentos.

Con todo, el problema mayor que suscita la información que de los usuarios obtienen estos rastreos es lo mucho que nos exponen al robo de identidad o fraudes *online*, que ya representa uno de los grandes frentes abiertos en la lucha contra la delincuencia a nivel internacional. La actividad delictiva que suscita el manejo de datos sobre numeraciones y contraseñas de tarjetas de crédito es cada día más sofisticada y compleja de combatir. Salvo los muy expertos, la inmensa mayoría de los navegadores no están en condiciones de conjurar esos riesgos y la sensación general es de desamparo.

"Libertad, ¿para qué?", decía Lenin, una frase tristemente célebre que algunos desaprensivos aplican ahora a la intimidad. Intimidad, ¿para qué?, coligen con descaro. Pues, aunque haya gente que ni siquiera la desea, la actividad en las redes viene a demostrar que, como poco, el preservar la intimidad nos permite vivir más seguro.