Entrevista a Raúl Siles*

* Analista de seguridad informática y socio fundador de Taddong

Hace unos meses se reunieron en Barcelona los principales expertos del mundo en seguridad de redes informáticas, en un evento conocido como Black Hat, acerca de la ciberdelincuencia y el software maligno. Entre los ponentes solo había un español, el analista Raúl Siles, socio fundador de Taddong, una compañía española que ofrece servicios avanzados de seguridad informática en todo el mundo. Es posible seguir sus investigaciones a través de su cuenta en Twitter, en el blog de la empresa y en su página personal. En esta entrevista, responde a algunas de las principales preocupaciones de los usuarios en materia de seguridad en Internet.

Fuente: eroski consumer

Autor: Por JORDI SABATÉ MARTÍ

28 de abril de 2011

¿Cuál es el punto más frágil en un ordenador: los puertos de conexión, la conexión a la Red, el sistema operativo?

Todos los componentes de un ordenador, tanto hardware como software, los han desarrollado personas y son potencialmente vulnerables a problemas de seguridad. En la actualidad, dos de los principales objetivos de los ataques informáticos, debido a su complejidad y sus numerosas vulnerabilidades de seguridad, son las aplicaciones web y las aplicaciones cliente más utilizadas, como los lectores de ficheros PDF, reproductores flash, Java, los navegadores web, reproductores multimedia, etc.

Por otro lado, no podemos olvidar que uno de los puntos más vulnerables aún es el usuario. Un buen ejemplo es el reciente incidente de seguridad en el que un atacante consiguió un nombre de usuario y contraseña válidos para generar certificados digitales asociados a una autoridad certificadora de confianza afiliada a la empresa Comodo. Como resultado, se generaron nueve certificados fraudulentos para sitios web de Google, Microsoft, Yahoo o Skype, que permitirían al atacante interceptar y manipular las comunicaciones seguras, en teoría, de cualquier usuario hacia estos sitios web.

¿Para proteger una red wifi es suficiente con una clave WEP, como las incluidas en las ofertas comerciales?

Los mecanismos de protección de las redes wifi basados en WEP crean una falsa sensación de seguridad. El hecho de tener que configurar y utilizar una contraseña de acceso a una red wifi puede hacer pensar al usuario que la misma es segura, sin ser consciente de que se conocen vulnerabilidades asociadas a WEP desde el año 2001 y que un atacante puede obtener la contraseña en menos de un minuto desde el año 2007. Por desgracia, todavía hoy en día muchos proveedores de telecomunicaciones y fabricantes configuran por defecto los puntos de acceso wifi con WEP, en lugar de usar la opción recomendada, WPA2, que debe usarse con claves bastante largas y que no sean fácilmente adivinables.

¿En general, es peligroso conectarse a Internet mediante una red wifi?

Si se configuran de manera adecuada, las redes wifi suponen un nivel de seguridad, en algunos casos, incluso superior a las redes cableadas. Es importante diferenciar entre tres tipos de escenarios muy comunes a día de hoy en la utilización de las redes wifi y sus niveles de seguridad. Una red wifi personal o corporativa, bien configurada con los mecanismos de seguridad disponibles en la actualidad -como WPA2, Personal o Enterprise- puede considerarse segura. Una red wifi pública compartida, configurada con los mismos mecanismos de seguridad anteriores, pero en la que todos los usuarios comparten el acceso, tiene problemas de seguridad debido a que, por su naturaleza, estas redes wifi están disponibles para el público en general. Cualquier usuario podría capturar y manipular el tráfico de otros usuarios. Para terminar, una red wifi pública compartida, abierta o insegura -sin cifrado, basada en WEP o en WPA2, pero con una clave fácilmente adivinable- es insegura, ya que cualquiera, incluso sin ser usuario de la red, podría capturar y manipular el tráfico de los usuarios legítimos.

Una de las tendencias del mercado es que el usuario pueda sincronizar de manera automática todos sus dispositivos a través de las redes de datos y mediante servidores. **¿Contribuiría esto a que una posible infección se extendiera de manera más rápida, como puede ocurrir en el parque informático de una empresa?**

En principio no, ya que los mecanismos de sincronización actuales se centran en permitir a un usuario compartir sus datos privados entre sus diferentes dispositivos, como su portátil y su teléfono móvil, y no en la compartición de datos entre usuarios. Sin embargo, este tipo de sincronización personal y la utilización de dispositivos móviles en mecanismos de autentificación más avanzados -como la validación de transferencias en la banca electrónica mediante un mensaje SMS enviado al teléfono del usuario- ha abierto la puerta a nuevos tipos de software malicioso. Su objetivo es infectar tanto el ordenador como el teléfono de la víctima para disponer de control sobre todos los elementos involucrados en validar la transacción financiera y poder así manipularla.

Los servicios en la llamada "nube" agrupan en una red de servidores concreta mucha información de sus clientes. **¿Se necesita un plus de seguridad para protegerlos?**

Sin duda, la externalización de servicios y tecnologías de la información hacia la "nube" requiere por parte de los usuarios y empresas un análisis muy exhaustivo de los mecanismos de seguridad asociados a las infraestructuras, tecnologías y procesos empleados por las compañías que proporcionan esta "nube". Este análisis no debe centrarse solo en las tecnologías más avanzadas, sino también en los principios básicos, como la seguridad física. En numerosas ocasiones, los servidores y redes que conforman la "nube" están ubicados en países extranjeros donde el nivel de seguridad en el acceso a los mismos es inferior al de la organización que hace uso de ellos.

Por otro lado, la agrupación de datos privados o sensibles en un mismo enclave tiene el riesgo de que un único incidente de seguridad podría comprometer los datos de múltiples entidades u organizaciones. Este tipo de incidentes los hemos vivido en numerosas ocasiones en el pasado con empresas de "hosting", donde se albergan los servidores y aplicaciones web de múltiples organizaciones, y, por desgracia, los volveremos a ver.

El nivel de cifrado simétrico de la tienda de Apple o de los servicios sensibles de Google es de RC4-128 bit. Otros servicios tienen niveles superiores, en concreto AES-256 bit. **¿Es suficiente con 128 bit o es mejor adoptar estándares superiores?**

Las afirmaciones respecto a la seguridad proporcionada por los algoritmos de cifrado y la longitud de las claves dependen mucho del momento temporal, de la capacidad de cálculo y de las posibles nuevas investigaciones en ese área. A día de hoy, las claves de cifrado simétrico de 128 bits todavía pueden considerarse seguras, un hecho ratificado por su amplia utilización en el comercio electrónico en Internet. Sin embargo, siempre es recomendable la adopción de estándares más avanzados, como AES frente a RC4, y de longitudes de claves mayores, siempre tras valorar el posible impacto en el rendimiento de la infraestructura y las aplicaciones que hacen uso de ellas. En el caso de los algoritmos de cifrado, el tamaño de las claves sí importa.

El problema no es tanto el algoritmo de cifrado empleado, sino la correcta utilización del mismo. RC4 se emplea tanto en HTTPS, para el acceso cifrado a la web, como en WEP, para el acceso, en teoría seguro, a las redes wifi. En el primer caso, el acceso mediante HTTPS y RC4 se considera lo bastante seguro y se emplea a diario en la banca y el comercio electrónico en Internet. En el segundo caso, el acceso mediante WEP y RC4 a las redes wifi es muy inseguro, debido a que el uso que se hace del algoritmo por parte de WEP es vulnerable, tal como especificaba en origen el propio diseño de RC4.

¿Son seguras las páginas web de los bancos y cajas desde donde gestionamos operaciones y transferencias?

Por desgracia, la seguridad no es un todo o nada. Es importante tener en cuenta la complejidad del software, y en concreto de las aplicaciones web, que utilizamos a diario para cualquier tarea de la vida cotidiana, como gestionar operaciones y transferencias bancarias en Internet, comprar viajes, entradas de espectáculos y otros productos. La complejidad y la seguridad no son muy buenos amigos, según mi experiencia y las auditorías de seguridad realizadas durante los últimos diez años, por lo que aún queda mucho que avanzar para disponer de aplicaciones web con un nivel de seguridad y protección elevado, si bien es cierto que las aplicaciones web de las entidades financieras son de las más seguras, debido a que la seguridad es un concepto intrínseco a ellas y a que disponen de mecanismos complementarios para la identificación y validación de transacciones sospechosas o fraudulentas.

¿Es seguro pagar con tarjeta de crédito en la página web de un comercio certificado y del cual el navegador asegura que cifra la conversación?

La industria informática, en concreto en lo que respecta a la seguridad, tiende a simplificar mucho los mensajes enviados a los usuarios para reducir la complejidad tecnológica que hay detrás. Por este motivo, es muy común ver el mensaje "este sitio web es seguro" en muchas páginas web, lo que indica solo que se emplea un certificado digital para cifrar las comunicaciones entre el usuario y la aplicación web. Además, muchos sitios web hacen uso de cifrado solo durante parte de la conversación, y no en su totalidad, lo que permite la realización de ataques para secuestrar la sesión del usuario en la aplicación web y suplantarle. Cualquiera puede obtener un dominio y espacio web en Internet por diez euros al año y adquirir un certificado digital, incluso, de forma gratuita.

Este mecanismo de cifrado, aunque necesario e imprescindible, solo protege frente a un número reducido de ataques, como la interceptación por parte de un atacante de las comunicaciones críticas del usuario, en las que se realiza el pago con la tarjeta de crédito. Hay numerosas vulnerabilidades de seguridad que afectan a las aplicaciones web de comercio electrónico y que no se solucionan mediante el cifrado de las comunicaciones, por lo que el mensaje transmitido al usuario es incompleto y puede ser engañoso. Por tanto, la utilización de un certificado digital no debería ser el único elemento que un usuario debe valorar al comprar con confianza en un sitio web de comercio elecrónico, sino que debería evaluar también la reputación de ese sitio web y la experiencia previa de otros usuarios.

¿Veremos software maligno en nuestros móviles ahora que aceptan arquitecturas complejas?

La respuesta no es si lo veremos, ya que en la actualidad hay numerosos ejemplos de software malicioso para múltiples plataformas móviles como iPhone, Symbian, Windows Mobile/Phone, Android, etc., sino cuándo su número superará al del software malicioso para los ordenadores. Creo que no es algo inminente. Los dispositivos móviles actuales son ordenadores completos en miniatura con las mismas capacidades, o incluso más, que los ordenadores portátiles o de sobremesa. Su capacidad de procesamiento, memoria, opciones de

conectividad -Bluetooth, wifi, 2G o 3G- y otras funcionalidades como GPS y cámara, junto con su vinculación al usuario las 24 horas y su uso en tareas cotidianas y sensibles, hacen de ellos un objetivo muy atractivo para el crimen organizado.

Para colmo, los mecanismos de seguridad disponibles hoy en los dispositivos móviles son similares a los que teníamos hace diez años en los ordenadores. En muchos dispositivos móviles no es sencillo para el usuario determinar si se conecta a una red wifi basada en WEP o WPA2, ya que lo único que puede ver es que la red tiene asociado el icono de un candado, por lo que debe ser segura. ¿O no? Del mismo modo, muchos de estos dispositivos móviles no permiten determinar si el acceso a un sitio web hace uso de cifrado mediante HTTPS, con lo que no es sencillo verificar los detalles del certificado digital empleado.

La penetración de la distribución de Linux Android en el mercado de los smartphones es espectacular. **¿Puede ser la puerta de entrada del software maligno en este sistema operativo?**

En efecto. La existencia de un número mayor de ataques o software malicioso para un sistema operativo en particular no depende tanto de la plataforma, sino de su adopción por parte de los usuarios y, por tanto, del retorno de la inversión que obtendrá el atacante. Todos ellos están basados en software potencialmente vulnerable y, de hecho, todos han presentado vulnerabilidades en el pasado y lo harán en el futuro.

En el caso concreto de Android, plataforma cuya seguridad analizamos en la actualidad, se difundió en marzo de 2011 a través de Android Market -la tienda de aplicaciones móviles de Android/Google- un conjunto de unas 50 aplicaciones que contenían un software malicioso denominado DroidDream. Como resultado, Google eliminó estas aplicaciones de la tienda y se vio obligado a utilizar su sistema de eliminación remota de aplicaciones de los dispositivos móviles de los usuarios -unos 200.000 según cifras no oficiales- que habían instalado alguna de estas aplicaciones y estaban, por tanto, infectados.

¿Debe considerar un usuario que su seguridad está en continuo peligro cuando navega por Internet o esto es una exageración?

En general, los usuarios sí deberían considerar que su seguridad está en entredicho al navegar por Internet, ya que la mayoría de usuarios utiliza Internet para acceder a múltiples sitios web, tanto de confianza como no. Una de las amenazas principales en Internet a día de hoy es que cualquier sitio web puede atacar al usuario, incluso los de confianza, ya que los atacantes logran comprometer estos sitios web y utilizarlos para extender el ataque a sus clientes. Esta afirmación está ratificada por el elevado número de ordenadores infectados en el mundo, tanto personales como corporativos, y la existencia de redes de ordenadores comprometidos controladas por atacantes.

En concreto, el navegador web y las aplicaciones cliente, o plugins, asociados a éste son uno de los objetivos principales de los atacantes y del crimen organizado en la actualidad. Debido a las numerosas vulnerabilidades en estos, y a versiones antiguas en los equipos de los usuarios, constituyen la puerta de entrada para tomar control del ordenador del usuario, de sus comunicaciones y de todas sus actividades en Internet.

¿Qué precauciones mínimas aconsejaría a un usuario para que su experiencia fuera segura?

- Los usuarios deberían seguir al menos las siguientes recomendaciones y buenas prácticas con el objetivo de aumentar su seguridad en la navegación web en Internet:
- Mantener el ordenador al día e instalar las últimas actualizaciones de seguridad disponibles para el sistema operativo.
- Mantener el navegador web actualizado a la última versión disponible. Es preferible utilizar las últimas versiones de los navegadores web, ya que disponen de mejoras de seguridad significativas, como Firefox 4, Internet Explorer 9, Chrome 10, Opera 11 o Safari 5.
- Mantener actualizadas a la última versión disponible todas las extensiones o plugins del navegador web asociadas a aplicaciones cliente muy utilizadas, como Adobe Reader, Adobe Flash, Java, o los reproductores multimedia Windows Media Player, QuickTime o RealPlayer.
- Acceder a los sitios web mediante HTTPS frente a HTTP, siempre que sea posible, es decir, en sitios web que soporten ambos. Utilidades como "HTTPS Everywhere", solo para Firefox, permiten automatizar el uso de HTTPS.
- Nunca se debe aceptar un certificado digital inválido en conexiones web cifradas HTTPS.
- No reutilizar la misma contraseña para diferentes sitios y servicios web.
- Utilizar dos ordenadores, dos máquinas virtuales, o al menos dos navegadores web para acceder a sitios web de distinta criticidad, como la navegación web ocasional o consulta de información y noticias, y la navegación web relevante de banca on line o compras en Internet.