Departamento de Seguridad Informática MINSAP

Enero 2017

Volumen 1, nº 1

Boletín de Seguridad Informática

Contenido:

Puntos de interés especial:

-Los servidores proxy anónimos nunca transfieren información que concierne a tu actual dirección IP.

-Adobe dedica el primer boletín de seguridad del año a las actualizaciones para Adobe Reader y Acrobat

-Los motivos para eliminar nuestra cuenta de un servicio web pueden ser varios, como por ejemplo:

.El servicio no respeta nuestra privacidad lo suficiente.

Sobre los Servidores Proxy Anónimos

¿Qué es un Servidor Proxy Anónimo?

Los servidores proxy anónimos nunca transfieren información que concierne a tu actual dirección IP. Esto significa que eres invisible en Internet. Ya que nadie tiene pistas sobre ubicaciones reales, no pueden establecer ninguna conexión ilegal con tu PC con el propósito supuesto de robar información confidencial o valiosa.

El hecho de que estés utilizando un servidor proxy a fin de conectarte a Internet puede ser tratado como un comportamiento normal en algunos casos. Es más, este servidor proxy anónimo ocultará tu verdadera IP con cuidado. En algunos casos para monitoreo, como el uso de Internet WAP, todos los usuarios son forzados a utilizar un servidor proxy en sus conexiones. Utilizar servidores proxy no siempre significa intentar esconderse.

Desventajas

Abuso. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.

Carga. Un proxy ha de hacer el trabajo de *muchos* usuarios.

Intromisión. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.

Incoherencia. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en cache sigue siendo la misma que la existente en el servidor remoto.

Irregularidad. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

Actualizaciones de seguridad para Adobe Flash Player, Acrobat y Reader

Adobe ha publicado dos boletines de seguridad para anunciar las actualizaciones necesarias para solucionar 13 vulnerabilidades en Flash Player y 29 en Adobe Acrobat y Reader.

Flash Player

El ya habitual boletín mensual para Flash, en esta ocasión el boletín APSB17-02 que soluciona 13 vulnerabilidades.

Los problemas incluyen cinco vulnerabilidades de corrupción de memoria, cuatro desbordamientos de búfer y tres por uso de memoria después de liberarla; que podrían permitir la ejecución de código. Por otra parte, otro problema de salto de medidas de seguridad que podría permitir la obtención de información sensible. Los CVE asignados son CVE-2017-2925 al CVE-2017-2928 y CVE-2017-2930 al CVE-2017-2938.

Adobe ha publicado las siguientes versiones de Adobe Flash Player destinadas a solucionar las vulnerabilidades, y se encuentran disponibles para su descarga desde la página oficial:

Flash Player Desktop Runtime 24.0.0.194

Flash Player para Linux 24.0.0.194

Igualmente se ha publicado la versión 24.0.0.194 de Flash Player para navegadores Internet Explorer, Edge y Chrome.

Adobe recomienda a los usuarios de Adobe Flash Player Desktop Runtime para Windows y Macintosh actualizar a través del sistema de actualización del propio producto o desde

http://www.adobe.com/go/getflash.

Para actualizar Adobe Flash Player para Linux:

http://www.adobe.com/go/getflash

Más información:

Security updates available for Adobe Flash Player

https://helpx.adobe.com/security/products/flash-player/apsb17-02.html

Security Updates Available for Adobe Acrobat and Reader

https://helpx.adobe.com/security/products/acrobat/apsb17-01.html

Adobe Reader y Acrobat

Adobe dedica el primer boletín de seguridad del año a las actualizaciones para Adobe Reader y Acrobat (boletín APSB17-01). Se han solucionado 29 vulnerabilidades que afectan a las versiones 15.020.20042 (y anteriores) de Acrobat DC y Acrobat Reader DC Continuous ,15.006.30244 (y anteriores) de Acrobat DC y Acrobat Reader DC Classic y Acrobat XI y Reader XI 11.0.18 (y anteriores) para Windows y Macintosh. Esta actualización soluciona una confusión de tipos, 12 problemas de corrupción de memoria, siete vulnerabilidades de uso de memoria después de liberarla y ocho desbordamientos de búfer; todos ellos podrían permitir la ejecución de código.

También se resuelve otro problema de salto de medidas de seguridad. Los CVE asociados son del CVE-2017-2939 al CVE-2017-2967. Adobe ha publicado las versiones 11.0.19 de Acrobat XI y Reader XI, Acrobat DC y Reader DC Continuous 15.023.20053 y Acrobat DC y Reader DC Classic 15.006.30279; las cuales solucionan los fallos descritos. Se encuentran disponibles para su descarga desde la página oficial, y a través del sistema de actualizaciones cuya configuración por defecto es la realización de actualizaciones automáticas periódicas.

Microsoft publica cuatro boletines de seguridad y soluciona 15 vulnerabilidades

Este martes Microsoft ha publicado cuatro boletines de seguridad (del MS17-001 al MS17-044) correspondientes a su ciclo habitual de actualizaciones y que según anunció son los últimos boletines que publica como tales. Según la propia clasificación de Microsoft dos de los boletines presentan un nivel de gravedad "*crítico*" mientras que los dos restantes son "*importantes*". En total se han solucionado 15 vulnerabilidades, 12 de ellas en Flash Player.

Tal y como anunció el pasado mes de noviembre, el mes que viene Microsoft no publicará esta serie de boletines informativos. Por el contrario, a partir del mes que viene utilizará una nueva base de datos de actualizaciones de seguridad, que ha dado en llamar "*Security Updates Guide*". Esto es, las actualizaciones seguirán publicándose, cambia la forma en que los usuarios obtendremos la información de los nuevos parches disponibles y los problemas corregidos.

Los boletines publicados son los siguientes:

MS17-001: Boletín "*crítico*" que incluye la también habitual actualización acumulativa para **Microsoft Edge**, el navegador incluido en Windows 10. En esta ocasión se soluciona **una vulnerabilidad** de elevación de privilegios si un usuario visita, con Microsoft Edge, una página web especialmente creada (CVE-2017-0002).

MS17-002: Boletín "*crítico*" destinado a corregir **una vulnerabilidad** si se abre un archivo específicamente creado con Microsoft Office (CVE-2017-0003).

MS16-004: Actualización considerada "*importante*" destinada a corregir una vulnerabilidad (CVE-2017-0004) de denegación de servicio en la forma en que Local Security Authority Subsystem Service (LSASS) trata las peticiones de autenticación. **MS16-003**: Como ya es habitual, Microsoft publica un boletín para resolver las vulnerabilidades solucionadas por Adobe en Flash Player en su también boletín periódico. Se trata de un boletín "*crítico*" que en esta ocasión soluciona **12 vulnerabilidades en Adobe Flash Player** instalado en Windows Server 2012, Windows Server 2016, Windows 8.1 y Windows 10; correspondientes al boletín APSB17-02 de Adobe (y que comentaremos con más detalle en una próxima una-al-día).

Las actualizaciones publicadas pueden descargarse a través de Windows Update o consultando los boletines de Microsoft donde se incluyen las direcciones de descarga directa de cada parche. Se recomienda la actualización de los sistemas con la mayor brevedad posible.

Se han anunciado múltiples vulnerabilidades en diferentes productos Kaspersky

Se ven afectados los productos:

– Kaspersky Anti-Virus 2016, 2017
– Kaspersky Internet Security 2016, 2017
– Kaspersky Total Security 2016, 2017
– Kaspersky Small Office Security 4, 5
– Kaspersky Fraud Prevention for Endpoints 6.0
– Kaspersky Safe Kids for Windows 1.1
– Kaspersky Endpoint Security for Mac

Los problemas fueron reportados por el conocido Tavis Ormandy de Google Project Zero. No es la primera vez que este investigador se centra en productos de seguridad, y más concretamente en Kaspersky. En esta ocasión **el problema reside en la característica de inspección de tráfico SSL/TLS que los antivirus Kaspersky usa** para detectar potenciales riesgos escondidos dentro de las conexiones cifradas.

Un usuario local puede obtener una llave privada empleada para gestionar conexiones SSL y **construir ataques contra las conexiones SSL** iniciadas por el navegador del usuario atacado.

Cuando el usuario atacado confía explícitamente en un certificado SSL no válido para un determinado sitio, es posible que un usuario remoto pueda omitir las advertencias de validación de certificados de los sitios enumerados en los Subject Alternative Names del certificado SSL no válido original.

Por último, un usuario remoto que pueda realizar un ataque de hombre en el medio podría aprovechar un error en la caché del certificado SSL para acceder a conexiones SSL iniciadas por el navegador del usuario de destino para un sitio.

La corrección se incluyo a través de la autoactualización el pasado 28 de diciembre. Se recomienda actualizar los productos afectados.

Más información:

Kaspersky: SSL interception differentiates certificates with a 32bit hash

Borrar tu identidad online no es imposible

Por lo general no somos conscientes de la gran cantidad de información personal que circula por la red. Borrar esa información puede convertirse en un problema, pero en el artículo de hoy, te enseñaremos a eliminar esta información en la medida de lo posible.

Redes sociales, servicios de mensajería, gestiones online, foros, comentarios en artículos, etc., hoy día nuestra identidad digital, datos y opiniones, pueden estar plasmados en multitud de servicios y sitios en Internet. En algunas ocasiones y en sitios en los que no quisiéramos, aparece nuestra información ya sea porque no lo valoramos en su momento o porque otro usuario lo copió y pegó en un sitio que desconocíamos. Sea como fuere, esa información aparece en Internet.

En primer lugar debemos tener claro qué queremos hacer: eliminar información concreta de algún sitio, eliminar una cuenta o eliminar una identidad completa.

1. Eliminar información concreta de un sitio.

En cualquier caso, el procedimiento para solicitar que alguien elimine información personal de un sitio es el siguiente:

-Contactar con el sitio web dónde está la información publicada y solicitar que la eliminen.
Si el sitio es español y después de haberlo solicitado el sitio web no la elimina, dirigirnos a la AGPD e interponer una denuncia.

En caso de que el sitio web no haga caso a nuestra solicitud o a la denuncia de la AGPD, deberemos poner una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.

2. Eliminar una cuenta.

Los motivos para eliminar nuestra cuenta de un servicio web pueden ser varios, como por ejemplo:

1. El servicio no respeta nuestra privacidad lo suficiente.
2. Cambio de los términos y condiciones de uso.
3. Hemos dejado de usar el servicio.

Deseo de modificar la orientación de nuestras publicaciones, por ejemplo asociar nuestro nombre a nuestra profesión y no a nuestro perfil personal.

En algunos servicios puede resultar un poco complejo eliminar nuestra cuenta. Si este es el caso, lo aconsejable es eliminar todo el contenido que podamos de manera manual. Para el resto, modificaremos nuestros datos personales, fotos e incluso crearemos contenidos que no tengan nada que ver con nosotros, para que encontrar información nuestra no sea tarea fácil.

3. **Eliminar nuestra identidad completa.**

Si nuestro objetivo es la eliminación total de nuestro rastro en Internet, el proceso será más o menos largo y complejo, en función de nuestro nivel de interacción con la red. Deberemos seguir una serie de pasos, y tener presente que la cuenta de correo será la última en borrar, ya que la necesitaremos para ciertas comunicaciones.

Borrar todas las cuentas.
Esta tarea también dependerá del nivel de interacción con la red, resultando así más o menos costosa. Primero debemos buscar todos los servicios en los que tengamos una cuenta creada. Habrá muchos de los que seamos conscientes, como Facebook, Twitter, Snapchat, Pinterest…Para buscarlas tendremos que mirar en nuestro correo electrónico, ya que cuando nos registramos en un servicio, el correo electrónico va asociado a esa cuenta, de forma que si buscamos en él, aparecerá alguno relativo a ese servicio siempre y cuando no hayamos eliminado los mensajes.

Modificar los perfiles de las cuentas que no se puedan borrar
Si hay algún servicio del cual no nos podemos borrar, o resulta demasiado complicado, debemos eliminar todo el contenido que podamos, modificaremos los datos del perfil, falseando los datos, cuidando de no implicar a terceros e incluyendo información “de relleno” para dificultar las búsquedas.

Eliminar las suscripciones a listas de correo
En los correos que nos envían periódicamente los servicios a los que nos hemos suscrito, nos indican como eliminar dicha suscripción. Para ello seguiremos las instrucciones, y en caso de no funcionar, lo comunicaremos al servicio a través de su soporte.

4. Conclusión.

Eliminar nuestros datos de Internet puede ser más simple o complejo en función de nuestra actividad o el tipo de información y los sitios donde se encuentre alojada, pero el derecho al olvido está para defendernos cuando pueda afectarnos de forma negativa.