2013-08-30

Boletín de Noticias de SeguridadInformática # 15

SCProgress

www.scprogress.com

ÍNDICE

NOTICIA 1: Google y su lucha contra el «malware»

Esta es una de las mayores preocupaciones de los internautas. El «malware» móvil es uno de los problemas informáticos que más ha crecido en el **segundo trimestre de 2013**, tanto en cantidad como en complejidad. Los cibercriminales no solo desarrollan programas cada vez más nocivos para plataformas móviles, sino que también están avanzando en capacidades y comportamiento de los programas. Por ello, es el equivalente a Windows en el mundo de los «smartphones».

Una iniciativa de Google trata de que el hecho de acceder a internet sea más seguro. Bajo esa premisa, cada semana la compañía publicará informes que informarán sobre las páginas web que no son seguras.

Y es que poco a poco el popular buscador se ha convertido en un

El gigante de internet localiza cada día 10.000 nuevas páginas web malintencionadas. Además, actuará contra la publicidad invasiva, la pornografía y los desnudos en Android

Jugador importante en la lucha contra el «malware», a juicio del experto en seguridad **Janus R. Nielsen** de la empresa de antivirus MySecurityCenter.

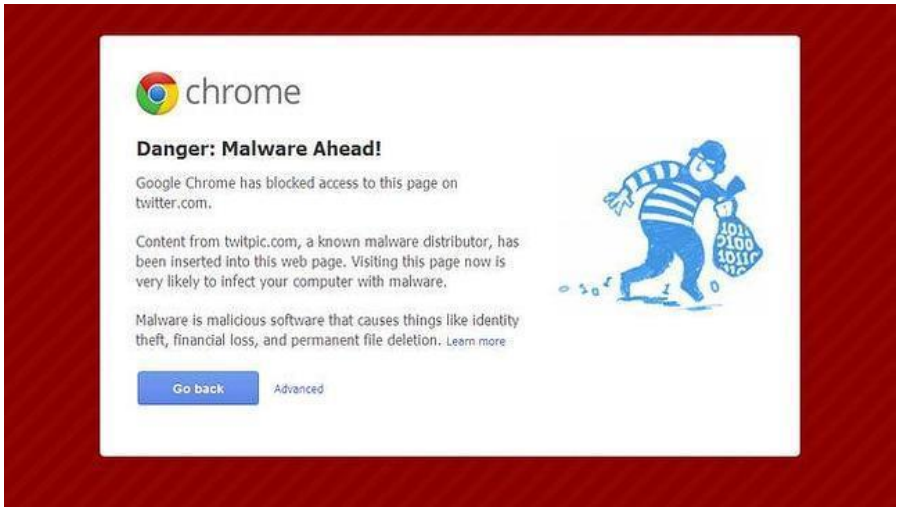
Cuando el informe de transparencia de Google fue lanzado en 2006, la compañía pretendía aumentar la transparencia en el motor de búsqueda más grande del mundo.

Además de mostrar que países y autoridades estaban aplicando censura en Google, ahora han añadido una sección del informe que muestra cuántos «malware» y sitios «phishing-infectados» se encuentran mediante la tecnología de **Google Safe Browsing, lanzado en 2008**.

«Esta iniciativa es un paso en la dirección correcta y creo que demuestra que Google reconoce su responsabilidad para mejor informar y proteger a los usuarios normales. Se encuentran cada día **10.000 nuevas páginas web malintencionadas**, que hace hincapié en el hecho de que el malware es un problema creciente», explica Nielsen.

Actualmente, el sistema de Google SafeBrowsing tiene registrados 1 billón de usuarios y con los nuevos informes se podrá ver cuántas advertencias Google emiten semanalmente (por ejemple la semana del 16 de Junio de 2013 hubo 88 millones). Estas advertencias incluyen «malware», donde los «hackers» pueden obtener acceso a tu PC y «phishing», que es un término para ataques donde los consumidores son engañados para que revele datos sensibles, tales como información de la cuenta.

Google también mostrará rápidamente cómo sitios web



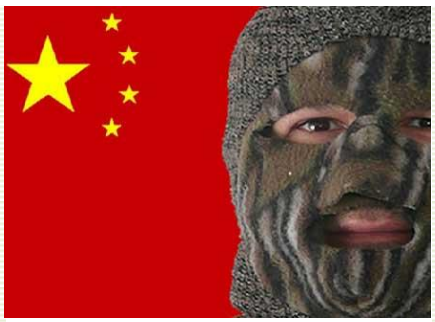
que han sido previamente infectado con «malware» se vuelven nocivos otra vez. «Ser consciente de que sólo Safe Browsing funciona en Chrome,Firefox y Safari, así que si utilizas Internet Explorer no obtendrá advertencias de Google pero sí desde el filtro SmartScreen de Microsoft. Sin embargo, uno puede fácilmente utilizar informes de Google para ver tendencias generales».

Un reciente informe de seguridad de programas de Microsoft indica que 25% de los usuarios de PC del mundo no tienen programas de antivirus instalado. «Esto indica que muchas personas todavía necesitan más información sobre las amenazas en línea y la seguridad de internet», explica este experto que hace hincapié en que los sistemas de protección de los navegadores no incluyen cortafuegos, que bloquean el tráfico inoportuno del ordenador antes de que acceda el virus.

En su lucha por un ambiente más «limpio» y obtener más calidad, Google ha introducido una serie de cambios en las políticas de la tienda Google Play para evitar la publicidad invasiva así como la existencia de pornografía y desnudos en su sistema operativo móvil Android, acusado de generar un flujo importante de «malware». En su lucha contra la pornografía, que le ha llevado incluso a evitar la entrada de este tipo de contenidos en su mimado dispositivo Google Glass, el gigante está creando una base de datos de imágenes que representan la explotación infantil.

Fuente: http://www.abc.es

NOTICIA 2: China sufre el mayor ataque DoS de su historia



China fue víctima del mayor ataque cibernético en su historia

En la madrugada del domingo, los internautas de China encontraron problemas de acceso a muchos servicios web del país. ¿El motivo? China sufrió el mayor ataque de denegación de servicio de su historia.

Aunque siempre nos haya parecido como algo sacado de una película made in Hollywood, Internet y las redes de comunicación se han convertido en un nuevo campo de batalla.

Casos como los de Stuxnet y la central nuclear de Irán, espionaje industrial o ataques de denegación de servicio son algunos ejemplos reales que hemos visto en estos dos últimos años. Países como Reino Unido, Estados Unidos o China cuentan con sus propios cibercomandos bien organizados y se dice que Rusia, por ejemplo, ha lanzado algún ataque contra países vecinos como parte de una "estrategia agresiva de negociación".

Si bien aún no se conoce muchos detalles al respecto, China, que normalmente suele ser origen de ciberataques,fue la victima de uno y durante la mañana de ayer el país se enfrentó al mayor ataque de denegación de servicio que han sufrido en su historia.

Creo que es importante partir de la base que China es un país en el Internet está limitado y servicios como Twitter o Facebook están limitados por el gobierno.

De hecho, existen redes sociales alternativas (como Weibo) que son las que son las que utilizan los internautas del país pero, a pesar de estas restricciones, estamos hablando de un mercado de 564 millones de Internautas que pueden hacer bastante ruido su sufren cortes de servicio.

Entre las 2 y las 4 de la madrugada del domingo, China sufrió un intenso ataque DoS que provocó deficiencias del servicio de acceso a Internet en el país y que, por ejemplo, fuese imposible acceder a páginas con dominio **.cn**. Aun así, la caída del servicio no fue total porque algunos sitios recurrieron a servir páginas cacheadas y también a servicios de CDN.

Fuente: http://noticias.seguridadpc.net

NOTICIA 3: 5 indicios de que tu cuenta fue pirateada

En una era en la que los delitos cibernéticos son cada vez más frecuentes y los hackers están cada vez más atentos para piratear nuestras cuentas en las redes sociales, los usuarios de las plataformas debemos estar atentos a ciertos cambios extraños en nuestro perfil.

Nosotros más que cualquier otra persona debemos proteger lo que es nuestro. Para ello, deberás valerte de ciertas recomendaciones y actuar si detectas algún cambio extraño en tu cuenta. Aquí repasaremos algunas modificaciones con las que puedes toparte y frente a las que deberás actuar, publicadas en el portal Baquia, en base a consejos de **AVIRA**:

1. Publicaciones ajenas que figuran como propias:

Si aparecen en la red mensajes enviados desde tu cuenta pero que nunca escribiste, inmediatamente bórralos y cambia tu contraseña.

Nuestro número de la cuenta bancaria y demás datos personales pueden estar en la red y los hackers usan tácticas cada vez más finas para ingresar a nuestros perfiles en las redes sociales y hacerse con nuestra información. ¡No lo permitas!

2. Alguien entra con una localización diferente:

Aunque dichos registros no son exactos, cuando alguien entra en tu cuenta desde un país muy alejado al tuyo saltará

3. Una aplicación publica en tu muro:

Si esto te sucede, puede que sea porque eres víctima de un likejacking, la técnica mediante la cual se disparan y distribuyen malwares a través de los "likes" a ciertas páginas. En este caso, lo ideal es que borres dichas publicaciones para que no vuelvan a aparecer en tu muro.

4. No puedes ingresar a tu cuenta

Si esto te ocurre, lo primero que debes hacer es intentar recuperarla. Si no puedes lograrlo, es probable que sea porque el hacker cambió el mail al que va asociado tu perfil. Cuando esto suceda, no te quedará otra alternativa que contactarte con la red ya sea Facebook, Twitter u otra, para que te ayude a recuperarla.

5. Sigues a personas que nunca aceptaste y ni siquiera conoces:

En estos casos, también es recomendable cambiar lo más rápido posible tu password. Otra opción es que tu cuenta envíe numerosos mensajes privados. En este caso, bórralos y advierte a tus contactos para que no abran ningún archivo que les hayas enviado.

Fuente: http://noticias.seguridadpc.net

NOTICIA 4: Cyberoam refuerza la seguridad de las Pymes Latinoamericanas

Cyberoam dio a conocer dos nuevos modelos de UTM's (Unified Treat Management, por sus siglas en Inglés) – CR200iNG y CR300iNG, diseñados para el mercado de la pequeña y mediana empresa. Siempre al ritmo de la evolución de las necesidades de las PyMes, y ante el actual panorama de amenazas cada vez más sofisticadas, los equipos CR200iNG y CR300iNG ofrecen la mejor protección de su clase, combinando software y herramientas de seguridad incluidas en la serie Cyberoam NG (Firewall para Aplicaciones Web, Control y Visibilidad de Aplicaciones, Controles basados en Identidad/Tecnología Capa 8, Protección Avanzada de Amenazas que comprende: Sistema de Prevención de Intrusos, AntiVirus/AntiSpyware Perimetrales, Protección AntiSpam Entrante y Saliente, Filtrado de Contenido Web y VPN).

De acuerdo a Marcelo Díaz, gerente general de makros, las

Los nuevos modelos Cyberoam cr200ing y cr300ing ofrecen seguridad avanzada y preparada para ataques futuros,

PyMEs son cada vez más receptivas para adoptar las nuevas tecnologías y nuevos modelos de negocio de TI. Además de la protección contra las más recientes amenazas de seguridad, buscan altos niveles de visibilidad, control y una mayor comprensión de su entorno de red, así como del comportamiento de los usuarios. "Las pequeñas y medianas empresas necesitan equipos de seguridad de alto rendimiento, controles basados en la Identidad, protección de aplicaciones contra amenazas avanzadas y soporte para tecnologías de alta velocidad como la 4G en un solo dispositivo. CR200iNG y CR300iNG ofrecen seguridad avanzada y preparada para ataques futuros, con un rendimiento que está a la par con los grandes dispositivos de seguridad corporativos", precisó.

Los dispositivos de la Serie NG vienen precargados con el sistema CyberoamOS – el firmware de Cyberoam más inteligente y potente que se haya desarrollado hasta la fecha. El nuevo firmware se integra perfectamente con el hardware de aceleración red y cifrado para ofrecer un alto rendimiento. El CyberoamOS también extrae el rendimiento completo de una plataforma multi-núcleo, junto con una latencia mínima, al tiempo que mejora la velocidad de procesamiento con el uso de tasas de interrupción optimizada y tecnología FastPath. La serie NG cuenta con procesadores a nivel Gigahertz para procesamientos de seguridad en nano segundos, y puertos tipo Gigabit Ethernet y de alta densidad.

Fuente: http://www.cioal.com