TOTALSEC NEWSLETTER – INFOSEC MX

BOLETIN No. 9

ABRIL 16 – 24

Elaboración: Abril 25, 2016

NEGOCIOS

En este número encontrarás noticias sobre:

- Negocios
- Aseguradoras
- Tecnología
- Gobierno

Panamá Papers: ¿Cómo lograron hackear a Mossack Fonseca?

por ABRIL 08, 2016 / PUBLIMETRO

De momento sin haber responsable directo, la empresa WordFence revisó los servidores de la firma Mossack Fonseca, encontrando un gran fallo.

La filtración pudo deberse a un plug-in desactualizado de WordPress y una versión antigua de Drupal, logrando con esto el acceso a la información del bufete de abogados.

La compañía estuvo enterada del problema durante un año y no corrigió las vulnerabilidades, empeorando la situación.

Mossack Fonseca contaba con dos sitios web principales, un mostrador de sus servicios en WordPress, y un portal de clientes con el objetivo de compartir información "delicada" a los mismos en Drupal.

Fuente: **http://www.publimetro.com.mx/tecno/panama-papers-como-lograron-hackear-a-mossack-fonseca/XeSpdh!FrHr3wqPaj9Zgijtkr9ARw/**

ASEGURADORAS

Protección contra hackers, el nuevo gran negocio de las aseguradoras

por ABRIL 19, 2016 / FORBES MEXICO

Xavier de Bellefon, CEO de Axa México, explica que debido a las grandes pérdidas por robo de información y suplantación de identidad, las aseguradoras revolucionarán para contar con seguros contra hackers.

Según datos de Alestra en México, se ha vulnerado a 5 de cada 6 empresas, y se calcula que el 40% de los mexicanos han sido blanco de un ciberataque.

La aseguradora AIG, estima que un fraude con información de los clientes implica una pérdida promedio de 2.6 millones de pesos para las empresas, resultando un peligro, ya que 87% carece de un protocolo de protección de datos.

Mientras Symantec indica que en 2015 este delito tuvo un costo para el país de 101,400 millones de pesos.

Fuente: **http://www.forbes.com.mx/proteccion-hackers-nuevo-gran-negocio-las-aseguradoras/**

Robo de identidad continúa en "alerta ámbar"

por MARZO 29, 2016 / SEGURIDAD INFORMATICA

Aseguradoras en México ofrecen ya coberturas en caso de robo de identidad, el semáforo que mide esta incidencia sigue en color "ámbar", implicando una etapa de prevención.

El director general de la Asociación Mexicana de Instituciones de Seguros (AMIS), Recaredo Arias, en la presentación de la 26 Convención de Aseguradores, expuso que la contratación de estos seguros no tiene aún un crecimiento importante porque en este momento se está en la etapa de alerta en riesgos, además, debe haber una gestión de riesgos y dentro de esto, el aseguramiento es una estrategia.

Fuente: **http://www.elsoldemexico.com.mx/finanzas/174615-robo-de-identidad-continua-en-alerta-ambar-advierten-aseguradoras**

TECNOLOGÍA

Linux se convierte en importante objetivo para los hackers

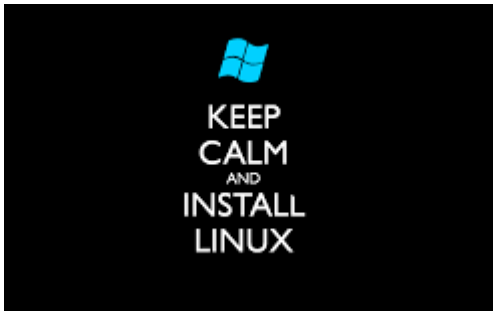
por ABRIL 07, 2016 / SILICON

Akamai ha lanzado una alerta sobre el aumento de los ataques contra ese sistema operativo de código abierto, ya que hackers están empleando malware enfocado a Linux para construir botnets que les permitan lanzar ataques de denegación de servicio (DDoS). Un ejemplo de esto es el troyano BillGates.

La compañía agregó que esos botnets han crecido en los últimos seis meses, teniendo una extensión de más de 100Gbps de tráfico para el lanzamiento de ataques.

Una vez que el malware infecta un ordenador, puede lanzar ataques DDoS, abrir puertos y servicios, llegando a tomar el control total del equipo.

Fuente: http://www.silicon.es/linux-se-convierte-en-importante-objetivo-para-los-hackers-2305485?utm_content=buffer8bfbe&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#BqYyu6TX86yUhLh4.99.



Proteger los archivos del smartphone es más fácil de lo que parece

por ABRIL 11,2016 / SIPSE

El proteger los archivos es sencillo dependiendo del software del dispositivo. Para la plataforma Android, se entra al ícono "Ajustes" y se selecciona la opción "Almacenamiento", para habilitar "Encriptación" del almacenamiento del teléfono, se recomienda que el teléfono esté conectado al toma de corriente o tenga al menos 80% de la batería, y cuando el proceso inicie, se ingresa una contraseña, además del PIN de acceso al equipo. Si se olvidan las contraseñas, la única forma de acceder nuevamente al móvil será restableciendo los datos de fábrica, pero toda la información se borrará.

Con el software iOS de iPhone, se tienen varias formas de resguardo, en la parte de "Configuración" en la opción de Touch ID y Código se puede incluir una contraseña de cuatro a seis dígitos y habilitar la opción de "Borrar Datos" al décimo intento de desbloqueo.

Así mismo, por medio del Touch ID se puede configurar las huellas digitales, una o varias. El dispositivo se puede conectar a una computadora y con iTunes podrá crear una copia de seguridad encriptada, lista para instalarse en un nuevo equipo.

Fuente: http://sipse.com/tecnologia/proteccion-datos-telefonos-inteligentes-ante-robo-199948.html

Hackers mejoran ataques ransomware dirigidos a servidores

por ABRIL 08, 2016 / COMPUTER WORLD MEXICO

El último método del que se valen los ciberdelincuentes para secuestrar dispositivos de organizaciones y empresas, es atacando servidores de aplicaciones Jboss que no han sido actualizados, para más tarde exigir un rescate.

El ransomware Samsam, se ha enfocado en infectar los equipos de organizaciones con la ayuda de la herramienta Jexboss y así aprovecharse de los servidores de la aplicación de Red Hat's JBoss.

Fuente: http://computerworldmexico.com.mx/hackers-mejoran-ataques-ransomware-dirigidos-a-servidores/

Cryptoworm, el rensomware que puede distribuirse por sí mismo

por ABRIL 13, 2016 / COMPUTO FORENSE

Expertos de seguridad de Cisco Talos, han descubierto que este malware está evolucionando para ser una amenaza más temida, ya que han observado que se está comenzado a utilizar el ransomware SamSam, apoyándose en una de las técnicas utilizadas por los virus que causaron conflictos entre los años 1990-2000, los gusanos.

Estos eran capaces de propagarse por sí solos para distribuirse por las redes de ordenadores, por lo que esta combinación da como resultado lo que Cisco nombró como Cryptoworm.

Fuente: http://www.computoforense.com/cryptoworm-el-ransomware-que-puede-distribuirse-por-si-mismo/

Jigsaw, el primer ransomware que elimina los archivos si no se paga

por ABRIL 12, 2016 / EL UNIVERSAL

Jigsaw cifra los datos de los usuarios para después pedir el pago de un rescate a cambio de recuperar el acceso a los mismos. Este malware reconoce más de 225 tipos de archivos, y utiliza el algoritmo AES para el cifrado, los ficheros resultantes tienen la extensión .fun

La diferencia con los otros ransomwares, es que pide el pago de 0.4 Bitcoin (alrededor de 3010.18 pesos) por la clave de descifrado, pero este informa que cada hora si no se hace el pago del rescate se eliminarán varios ficheros secuestrados de manera aleatoria, aunque el usuario reinicie, se ha reportado que han llegado a eliminar más de 1000 archivos.

Investigadores de seguridad han proporcionado la herramienta Jigsaw Decrypter Ransomware, la cual se puede descargar de forma gratuita. Es detectada como aplicación sospechosa por algunos antivirus, pero es totalmente fiable y efectiva para la recuperación de datos de este ransomware.

Fuente: http://www.redeszone.net/2016/04/12/jigsaw-primer-ransomware-elimina-los-archivos-no-se-paga/?utm_content=buffer2f439&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

GOBIERNO

Casa de Moneda ve más ciberataques

por ABRIL 11, 2016 / EL UNIVERSAL

La Casa de Moneda alerta sobre el crecimiento de ataques informáticos contra entidades públicas y compañías en México, donde el activismo seguirá siendo parte fundamental de este tipo de ataques, ya que crece el número de seguidores.

Indica también que el 46% de las empresas no invierte en plataformas integrales en seguridad informática, y no tiene personal calificado, por lo que estos incidentes se incrementaron un 300% costando al país millones de pesos al año.

En el análisis costo-beneficio para desarrollar la Plataforma de Seguridad Informática e Inteligencia Corporativa para La Casa de Moneda de México, propuesta remitida a la Secretaría de Hacienda y Crédito Público para su aprobación y con la espera a obtener 14.4 millones de pesos para su implementación, ya que según el documento este organismo carece tanto de personal calificado como de la tecnología para confrontar estos problemas.

Fuente: http://eluniversal.com.mx/articulo/cartera/finanzas/2016/04/11/casa-de-moneda-ve-mas-ciberataques

SAT alerta sobre correo fraudulento

por ABRIL 18, 2016 / SIPSE

Nuevamente El Servicio de Administración Tributaria (SAT), manda una alerta a los contribuyentes sobre correos apócrifos enviados en su nombre, por lo que recomendó no descargar archivos ni compartir información a través de estos.

En su cuenta en Twitter, el SAT publicó: "¡Atento! El correo 'notificaciones@sppld.sat.gob.mx', envía mensajes falsos en nuestro nombre, no compartas tus datos".

El SAT recordó que las autoridades tributarias solo les envían mensajes a través del Buzón Tributario, ofreciendo seguridad en el intercambio de información entre las partes.

Fuente: http://sipse.com/mexico/sat-alerta-sobre-correo-fraudulento-201041.html

CONDUSEF da a conocer nuevo caso de phishing

por ABRIL 15, 2016 / CONDUSEF

Comunicado No. 032

Detecta correo electrónico apócrifo de Bancomer.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), pide a los usuarios de banca electrónica no dejarse engañar por un nuevo correo electrónico apócrifo de Bancomer en donde solicitan actualización de datos a clientes por medio de un falso correo en el que se solicita al usuario actualizar sus datos debido a cambios en la plataforma de "Bancomer Alertas", de lo contrario, no podrá acceder a los servicios de banca en línea de manera correcta.

Este correo proporciona ligas que llevan al usuario a un sitio falso en donde solicitan su información personal, como contraseñas, número de identificación personal (NIP), número de cuenta bancaria, etc.

Por lo que CONDUSEF recuerda que ni las entidades financieras, ni VISA o MasterCard, solicitan datos personales a sus clientes o verificación de sus cuentas mediante correo electrónico. Por lo que se deben tomar las precauciones pertinentes.

Fuente:
http://www.condusef.gob.mx/index.php/prensa/comunicados-2016/1314-condusef-da-a-conocer-nuevo-caso-de-phishing

TOTALSEC NEWSLETTER - INFOSEC

BOLETÍN No. 9

16 - 24 ABRIL, 2016

Elaboración: ABRIL 25, 2016.