NEWSLETTER – INFOSEC MX

BOLETIN No. 12

MAYO 07-15

Elaboración: Mayo 16, 2016

FINANZAS

En este número encontrarás noticias sobre:

- Finanzas
- Tecnología
- Legal
- Gobierno

Aumentan 15% los fraudes en cajeros automáticos

por MAYO 10 2016 / ABC TECNOLOGÍA

El Centro Europeo de Ciberdelincuencia de Europol (EC3) y Trend Micro alertan sobre cómo los grupos criminales han visto que el uso de 'malware' es la forma más fácil y segura de robar dinero e información de las tarjetas bancarias. Además, dichos fraudes se incrementaron en un 15% entre el 2014 al 2015.

Para esto, los criminales utilizan cada vez más las herramientas de hackeo. Los principales países afectados según la European ATM Security Team, es EE.UU., Indonesia y Filipinas. Uno de los factores que facilitan este delito es que Windows XP ya que no puede recibir los parches de seguridad, además los expertos aseguran que también la falta de medidas de seguridad por parte de los bancos en América Latina y Europa del este han abierto la puerta para este ataque a los cajeros automáticos, estas técnicas se están exportando a otros países ampliando la cantidad de ataques.

Fuente: http://www.abc.es/tecnologia/redes/abci-ciberataques-cajeros-automaticos-tendencia-auge-201605092058_noticia.html

TECNOLOGÍA

En Morelos ya se castiga el delito de suplantación de identidad

por MAYO 09, 2016 / LA UNIÓN

Morelos se convirtió en la quinta entidad al incorporar en su legislación penal el delito de suplantación de identidad, entrando en vigor la adición del Capítulo V BIS, y del Artículo 189 Bis del Código Penal para el Estado, estableciendo lo siguiente:

"Al que, por cualquier medio suplante la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la suplantación en su identidad, causando con ello un daño o perjuicio u obteniendo un lucro indebido, se le impondrá una pena de uno a cinco años de prisión, de cuatrocientos a seiscientos días de multa y, en su caso, la reparación del daño que se hubiere causado".

Fuente:
http://www.launion.com.mx/morelos/sociedad/noticias/89080-en-morelos-ya-se-castiga-el-delito-de-suplantacion-de-identidad.html

Crean una nueva app que detecta si tu iPhone ha sido hackeado

por MAYO 10, 2016 / APPLESFERA

Stefan Esser, analista de seguridad, creó Systems and Security Info, que es una aplicación de pago que alerta al usuario ante jailbreaks, además analiza la actividad del móvil para detectar comportamientos sospechosos. El proceso del jailbreak permite que aplicaciones no aprobadas por Apple, se ejecuten, además, es la puerta de entrada para que puedan instalarse aplicaciones y se ejecuten sin que el usuario lo sepa.

También con esta app se puede comprobar si hay malware instalado con un análisis indicando si la terminal está afectada o limpia. Esta aplicación está disponible en la App Store a un precio de 0,99 euros (20.30 pesos aproximadamente).

Fuente: http://www.applesfera.com/aplicaciones-ios-1/crean-una-app-que-detecta-si-tu-iphone-ha-sido-hackeado

"Ciberseguridad" será prioritaria para el 78% de organizaciones en México: CompTA

por MAYO 09, 2016 / CIO MEXICO

La organización CompTIA realizó un estudio en México y otros 11 países la cual arrojó que el 79% de las compañías esperan que la ciberseguridad sea una prioridad en los próximos dos años. Esto debido a que casi tres de cada cuatro organizaciones han sido víctimas de algún incidente o violación de ciberseguridad durante el último año, y de las violaciones el 60% se consideraron como serias.

En el estudio International Trends in Cybersecurity, se encuestaron a más de 1,500 ejecutivos en 12 países, mostrando que el 73% de las organizaciones sufrieron una violación o incidente en el mismo lapso de tiempo. Estas violaciones se observaron mayormente en India (94%), Malasia (89%), Brasil (87%), México (87%) y Tailandia (82%). Siendo Japón (39%) y Emiratos Árabes Unidos (40%), los que menos incidentes tuvieron. Los incidentes de seguridad relacionados con móviles fueron más altos: un promedio de 76% en los 12 países, México con (80%), Tailandia (95%) e India (91%) fueron los más altos.

Fuente: http://cio.com.mx/ciberseguridad-sera-prioritaria-para-78-de-organizaciones-en-mexico-comptia/

Google retira casi 200 aplicaciones Android infectadas con malware

por MAYO 09, 2016 / GLOBB SECURITY

Esto a raíz de los sucesos recientes como el del hacker Andrés Sepúlveda que afirmó haber participado en las últimas elecciones presidenciales alterando el curso de las campañas por medio del uso de malware, bots o ciberespionaje. Así mismo, la filtración del padrón electoral del INE con los datos de 93 millones de electores. Se le está prestando atención a las campañas políticas que están por venir, esto debido a la ausencia de medidas de protección, o el mal manejo de los datos, que puede perjudicar a todos.

La ciberseguridad debe formar parte de las estrategias de campaña de los candidatos para evitar algunos ataques como ataques publicitarios, espionaje o minimización de la participación de un adversario político, por ejemplo, comprometiendo sus cuentas. Así como la sustracción de información sensible como discursos políticos, reuniones, programas y estrategias de campaña.

Fuente: http://globbsecurity.com/google-retira-190-aplicaciones-infectadas-38303/

Si utilizas Tor o VPN, eres sospechoso para Estados Unidos

Por MAYO 02, 2016 / COMPUTER HOY

El uso de estas herramientas en cualquier país podría generar un problema con el gobierno de los Estados Unidos, esto si se aplica la última modificación de la Regla 41 de las Federal Rules of Criminal Procedure. De ser aprobada, jueces de ese país podrían autorizar el acceso remoto a los dispositivos que utilicen herramientas de privacidad. Así mismo quien desactive la ubicación de su dispositivo también se consideraría sospechoso, por lo que se podría ordenar el acceso remoto a su dispositivo, su incautación e incluso hacer la copia de todo lo que tenga almacenado.

La Fundación Fronteras Electrónicas (EFF), cuyo fin es conservar los derechos de la libertad de expresión en la era digital, advierte que, de aprobarse esa modificación, también los dispositivos víctimas de malware serán objetivo aún sín autorización de los dueños para tratar de identificar la fuente de estas redes. Esta iniciativa ya pasó por la 'Corte Suprema de los Estados Unidos de América', e irá al Congreso, para ver si se aprueba.

Fuente: **http://computerhoy.com/noticias/internet/si-utilizas-tor-vpn-eres-sospechoso-eeuu-44246**

El cambio de política para VirusTotal hará más vulnerable a la industria del software

por MAYO 09, 2016 / SILICON

Startups de seguridad están perdiendo el acceso a la colección de análisis de virus informáticos, el servicio se cortó sin previo aviso a empresas que no comparten evaluaciones de muestras detectadas debido a que empresas de Seguridad, algunas con valoraciones de más de 1.000 millones de dólares no han aportado su análisis sobre infecciones. Las grandes empresas del sector, algunas con valoraciones más pequeñas, han presionado para esta acción.

Analistas del mercado y directivos de algunas compañías afirman que esto llevará a que algunos servicios clasifiquen erróneamente software legítimo como maliciosos y tengan menor capacidad de proteger a sus clientes de las amenazas, al menos en el corto plazo. Google ejecuta la base de datos de VirusTotal para que profesionales de Seguridad puedan compartir ejemplos de software y opiniones sobre el malware.

Fuente: **http://www.silicon.es/el-cambio-de-politica-de-virustotal-hara-mas-vulnerable-a-la-industria-del-software-2308049**

Abril de 2016 ha sido el peor mes en cuanto a amenazas de ransomware

por MAYO 06, 2016 / REDES ZONE

Kaspersky ha detectado en el primer trimestre de 2016, más de 2900 nuevas variantes de este malware, creciendo un 14% respecto al 2015. Considerando que la base de datos de Kaspersky tiene 15.000 entradas, en ese periodo se han añadido alrededor del 20% de estas. El laboratorio ha detectado y bloqueado más de 370.000 ataques de ransomware, 17% de estos direccionados a empresas.

Según informes, el pasado mes de abril aumentó la actividad de este malware en un 19%, siendo este probablemente en el peor mes de la historia de este tipo de malware. El mayor número llega a los usuarios a través de correos electrónicos de SPAM o descargas maliciosas desde páginas web, por lo que, al no ejecutar los archivos adjuntos o no hacer las descargas, el riesgo se reduciría bastante. Además de eso, ayudaría mantener el sistema operativo y todos los programas actualizados, un buen antivirus y evitar visitar webs sospechosas.

Fuente: **http://www.redeszone.net/2016/05/06/abril-2016-ha-peor-mes-cuanto-amenazas-ransomware/?utm_content=buffer22dc8&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

El ransomware Locky, ahora cifra las comunicaciones con el servidor de control

por MAYO 03, 2016 / REDES ZONE

Con este ransomware, los ciberdelicuentes eliminaron la comunicación entre los extremos, por lo que se necesitará una clave privada RSA para poder tener acceso al interior de la red, aparte de la clave pública que ya se distribuía. Antes, la amenaza distribuía una clave pública única a cada usuario infectado formando parte del proceso de cifrado de los archivos. A partir de ahora será necesaria la clave privada para extraer el contenido de las peticiones y respuestas realizadas entre el equipo del usuario y el servidor de control, algo muy complicado.

El objetivo es dificultar las tareas de los expertos en seguridad al extraer información sobre la amenaza y desarrollar un software para el descifrado de la información. A los ciberdelincuentes con esta modificación les permite conocer la dirección IP del equipo infectado, pero no la que se envía y recibe. También buscan proteger el servidor de accesos no autorizados y evitar que este sea utilizado para distribuir otras amenazas y que otros se beneficien a costa de su infraestructura.

Fuente: **http://www.redeszone.net/2016/05/03/ransomware-locky-ahora-cifra-las-comunicaciones-servidor-control/**

Evite Pagar rescate por dispositivos

por MAYO 09, 2016 / AM

Según la firma Cyber Threat Alliance, a nivel internacional se pagaron alrededor de 325 millones de dólares en 2015 por el rescate de dispositivos bloqueados y cifrados por ciberdelincuentes. Especialistas en Seguridad recomiendan no realizar el pago ya que no existe garantía de tener los archivos de vuelta. Este software malicioso se encuentra a la venta como un servicio, por lo que cualquier persona puede, sin muchos conocimientos técnicos, comprarlo y darle un uso delictivo.

Para evitar un ataque se recomienda usar software original, ya que el software pirata abre la puerta para que delincuentes aprovechen vulnerabilidades. En cuanto a un ataque a móviles, puede ser sólo un bloqueo que al reiniciar el equipo se reestablece. En el caso de las computadoras se necesita acudir a un especialista para solucionarlo. Al ser atacado, es probable que el delincuente haya accedido a información sensible, por lo que es recomendable cambiar todas las claves y no usar la misma para todos los servicios.

Fuente: http://www.am.com.mx/2016/05/09/tecnologia/evite-pagar-rescate-por-dispositivos-282757

LEGAL

Suprema Corte de México aprueba la retención de metadatos, intervendrá la CIDH

por MAYO 05,2016 / ARISTEGUI NOTICIAS

La Suprema Corte de Justicia de la Nación (SCJN), tomó la decisión final sobre el amparo contra los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), que fue negarse al amparo solicitado por la Red en Defensa de los Derechos Digitales (R3D) contra los apartados de la LFTR, legalizando así la conservación masiva de metadatos de comunicaciones de los usuarios mexicanos por un periodo de dos años, y tener el acceso a estos las instancias de justicia y Seguridad del país.

Se retendrán datos como identidad, origen, destino, hora y duración de las comunicaciones, además, se considerará legal aplicar seguimientos con geolocalización en tiempo real sin la necesidad de una autorización judicial. Por su parte, Luis Fernando García, director de R3D dijo que, ya que se agoten todas las instancias en el derecho interno, se recurrirá a la Corte Interamericana de Derechos Humanos (CIDH) para que evalúe y decrete su postura sobre el tema.

Fuente: http://aristeguinoticias.com/0405/mexico/valida-corte-conservar-datos-de-usuarios-de-telecomunicaciones/

GOBIERNO

Alerta CONDUSEF por robo de identidad

por MAYO 03, 2016 / CAPITAL HIDALGO

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), delegación Hidalgo, dio un aviso a la población sobre el aumento en el robo de identidad. En el primer trimestre del año, hubo 504 controversias, de las cuales 73 fueron por posible robo de identidad, dando esto un 14% de los delitos registrados por la dependencia.

De esas 73 controversias, 51 son por crédito no reconocido en el historial crediticio, 12 son por inconformidad con el cobro de productos o servicios no contratados por el usuario, 6 por créditos otorgados sin ser solicitados ni autorizados por el interesado, 3 en las que el interesado no reconoce haber celebrado contrato con la institución y sólo 1 por apertura de cuenta no solicitada ni autorizada por el interesado.

Fuente: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad

TOTALSEC NEWSLETTER - INFOSEC

BOLETÍN No. 12

MAYO 07-15, 2016

totalsec
Security Operation Center